KTI NETWORKS

KGS-2422

Web Management Interface

User's Manual

DOC.120308

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:

United States KTI Networks Inc.
P.O. BOX 631008
Houston, Texas 77263-1008

United States	Phone:	713-2663891
	Fax:	713-2663893
	E-mail:	kti@ktinet.com
	URL:	http://www.ktinet.com/
International	Fax:	886-2-26983873
	E-mail:	kti@ktinet.com.tw
	URL:	http://www.ktinet.com.tw/

Table of Contents

1. Web Management

The switch features an http server which can serve the management requests coming from any web browser software over TCP/IP network.

Web Browser

Compatible web browser software with JAVA script support

Microsoft Internet Explorer 7.0 or later

Set IP Address for the System Unit

Before the switch can be managed from the web browser software, make sure a unique IP address is configured for the switch.

1.1 Start Browser Software and Making Connection

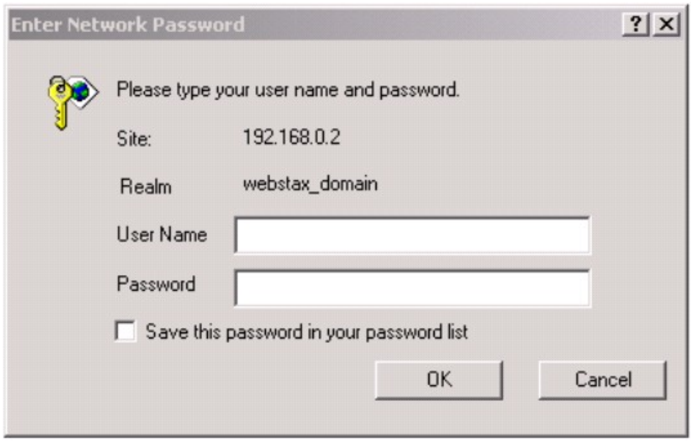
Start your browser software and enter the IP address of the switch unit to which you want to connect. The IP address is used as URL for the browser software to search the device.

URL: http://xxx.xxx.xxx.xxx/

Factory default IP address: *192.168.0.2*

1.2 Login to the Switch Unit

When browser software connects to the switch unit successfully, a Login screen is provided for you to login to the device as the left display below:



Please type your user name and password.

Site: 192.168.0.2

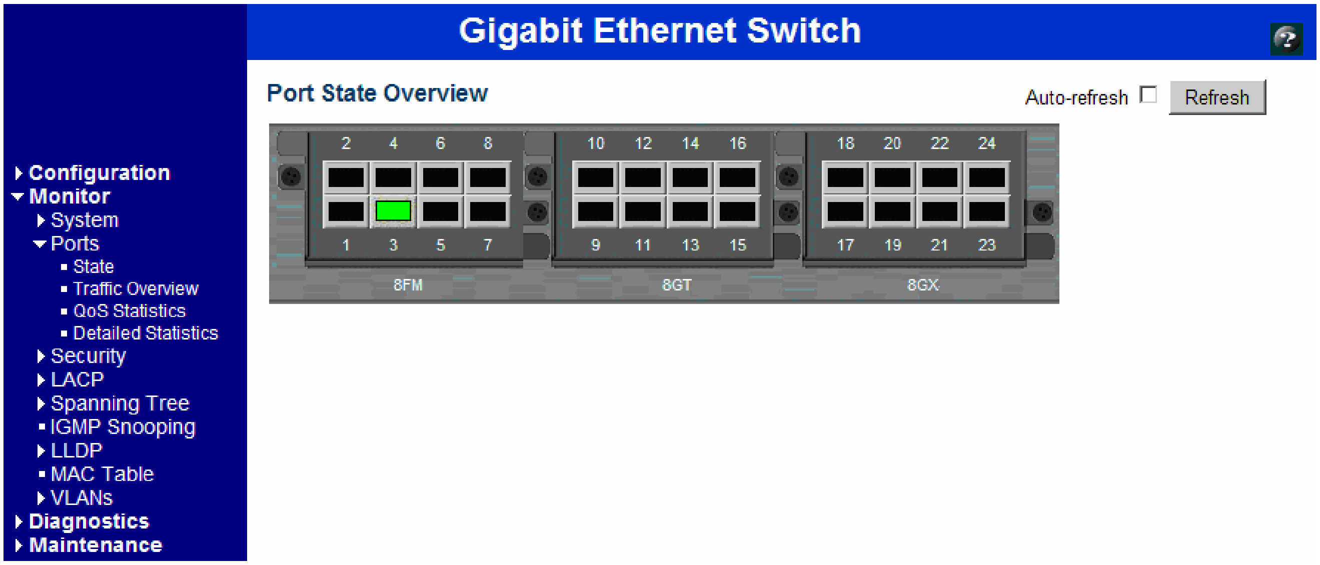
Realm webstax_domain

User Name

Password

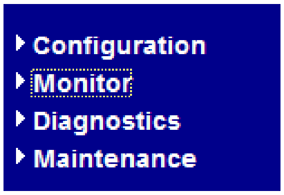
□ Save this password in your password list

The switch will accept more than one successful management connection at the same time. A switch image icon is displayed as follows after a successful login. The following example shows an image of a 24-port switch model.

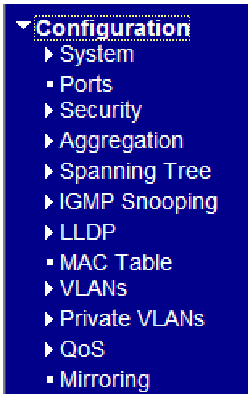


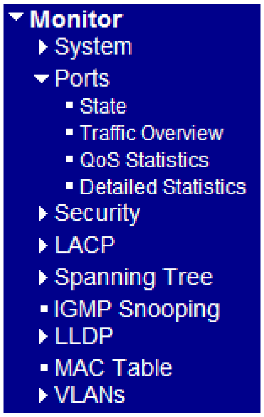
1.3 Main Management Menu

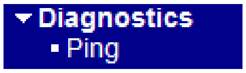
Main Menu:

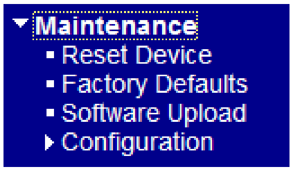


Sub-menus:









Configuration

System	Switch information, IP configuration, SNTP setting, and Password setting
Ports	Port operation related configuration, frame size, and power saving control
Security	Switch & UI authentication configuration, Port access security control
Aggregation	LACP port link aggregation related configuration
Spanning Tree	STP bridge, MSTI and CIST configuration
IGMP Snooping	IGMP basic and port configuration
LLDP	LLDP configuration
MAC Table	MAC address learning settings and static MAC address port configuration
VLANs	VLAN groups and VLAN port-related configuration
Private VLANs	PVLAN groups and port isolation configuration
QoS	QoS port ingress, egress and QCL configuration, Port rate control, QCL wizard
Mirroring	Port mirroring settings

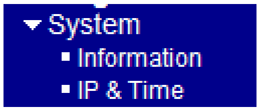
Monitor

System	System information and system log information
Ports	Port link status, traffic statistics, QoS statistics
Security	Switch & UI authentication, Port access security status
LACP	LACP system and port status
Spanning Tree	Bridge status, Port status and RSTP/STP/MSTP statistics
IGMP Snooping	IGMP groups learned, Router ports, Statistics

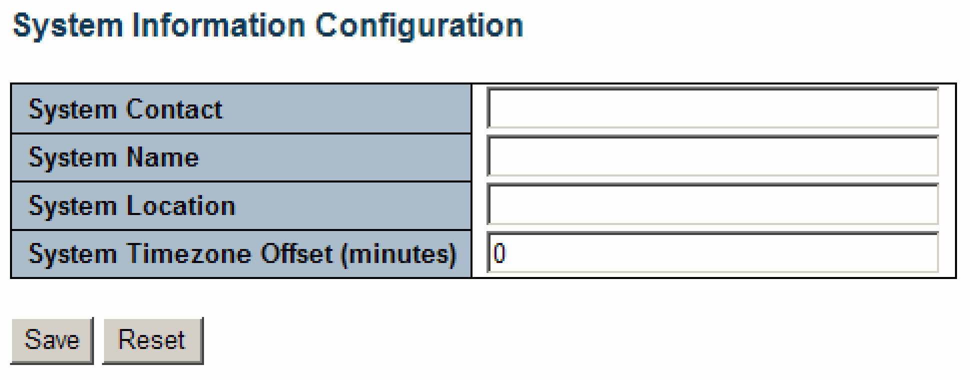
LLDP	LLDP neighbors information, Port statistics
MAC Table	Display of MAC address table
VLAN	Display VLAN membership and VLAN port status
Diagnostics	
Ping	ICMP ping utility
Maintenance	
Reset Device	Command to reboot the switch
Factory Defaults	Command to restore the switch with factory default settings
Software Upload	Command to update the switch firmware
Configuration	Command to save or upload the system configuration

2. Configuration

2.1 System



2.1.1 Information



System Information Configuration

System Contact	
System Name	
System Location	
System Timezone Offset (minutes)	0

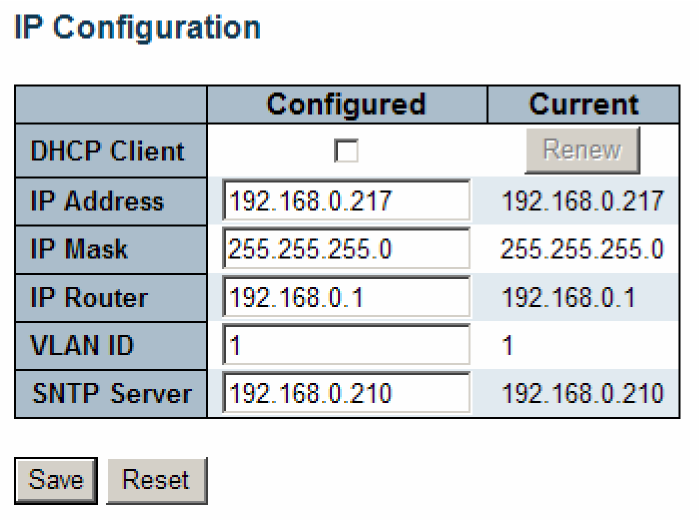
Configuration	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is *0* to *255*, and the allowed content is the ASCII characters from *32* to *126*.
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is *0* to *255*.
System Location	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is *0* to *255*, and the allowed content is the ASCII characters from *32* to *126*.
System Timezone Offset	Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. Valid range: *-720* to *720* minutes.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Note:

1. *It is suggested to give each switch unit a system name as an alternative unique identification beside IP address.*

2. The system Name, Contact, and Location settings are also used as SNMP MIBs.

2.1.2 IP & Time



IP Configuration

	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.0.217	192.168.0.217
IP Mask	255.255.255.0	255.255.255.0
IP Router	192.168.0.1	192.168.0.1
VLAN ID	1	1
SNTP Server	192.168.0.210	192.168.0.210

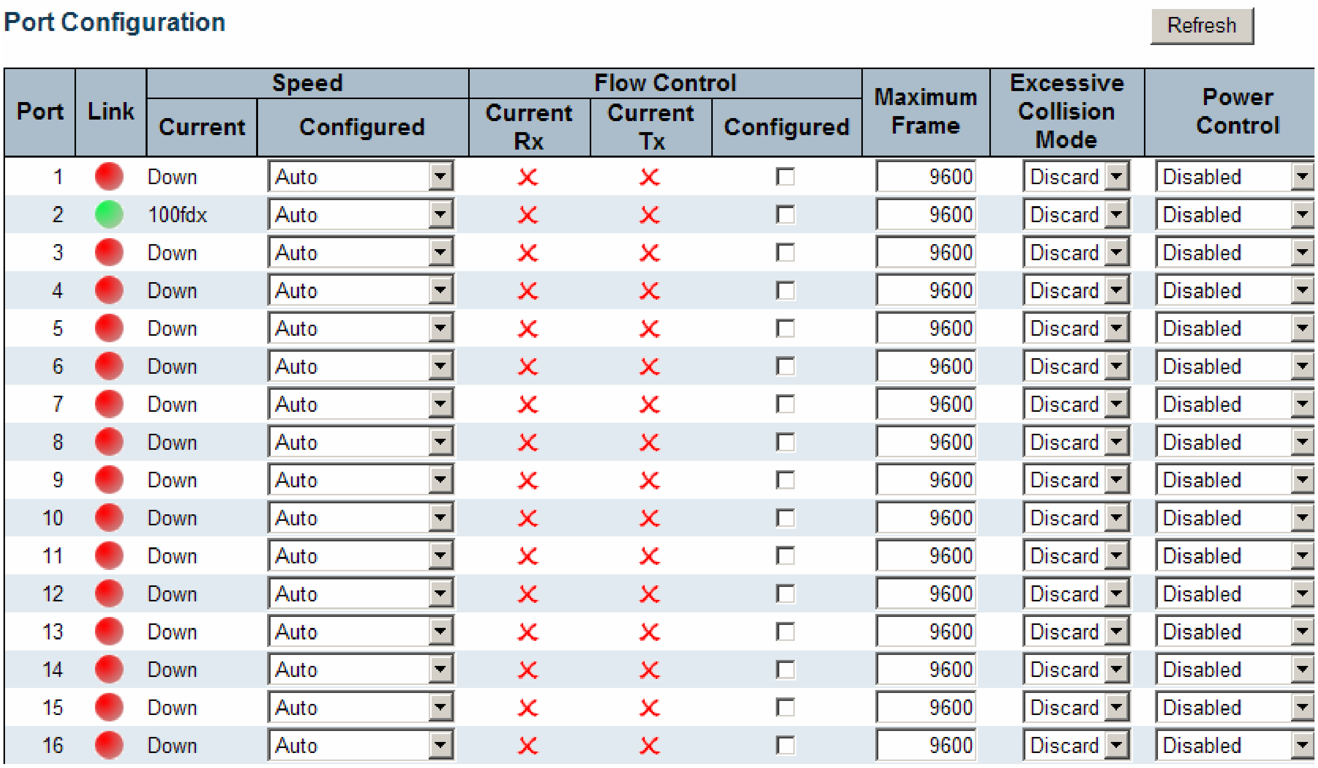
Configuration	Description
DHCP Client	Enable the DHCP client by checking this box.
IP Address	Provide the IP address of this switch unit.
IP Mask	Provide the IP mask of this switch unit.
IP Router	Provide the IP address of the default router for this switch unit.
VLAN ID	Provide the managed VLAN ID. The allowed range is *1* through *4095*.
SNTP Server	Provide the IP address of the SNTP Server.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.

Note:

1. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

2. The IP addresses should be in dotted decimal notation.

2.2 Ports

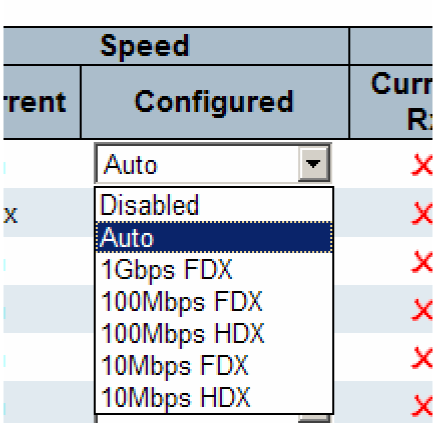


Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
1	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
2	🟩	100fdx	Auto	✗	✗	□	9600	Discard	Disabled
3	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
4	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
5	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
6	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
7	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
8	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
9	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
10	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
11	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
12	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
13	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
14	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
15	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled
16	🟥	Down	Auto	✗	✗	□	9600	Discard	Disabled

Configuration	Description
Port	The port number associated to this configuration row
Link	The current link status is displayed graphically. Green indicates the link is up and red that it is down.
Speed - Current	Provides the current link speed of the port.
Speed - Configured	Select any available link speed for the given switch port.

Options for 10/100/1000M Copper port type:



Disabled: disables the switch port operation.

Auto: selects the highest speed that is compatible with a link partner.

1Gbps FDX: selects auto-negotiation 1000Mbps and full duplex

100Mbps FDX: selects fixed 100Mbps and full duplex

100Mbps HDX: selects fixed 100Mbps and half duplex

10Mbps FDX: selects fixed 10Mbps and full duplex

10Mbps HDX: selects fixed 10Mbps and half duplex

Options for 100/1000M Pluggable SFP port type:

Disabled: disables the switch port operation.

Auto: Auto-negotiation., 1000M and full duplex

100Mbps FDX: selects fixed 100Mbps and full duplex

Options for Fixed 100M Fiber port type (ST, SC, BiDi, VF-45):

Disabled: disables the switch port operation.

100Mbps FDX: selects fixed 100Mbps and full duplex

Flow Control – Current Rx
Whether pause frames on the port are obeyed

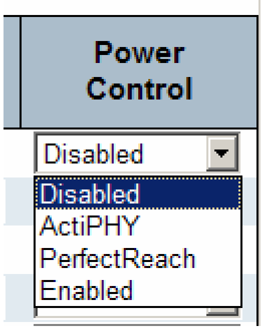
Flow Control – Current Tx
Whether pause frames on the port are transmitted

Flow Control – Configured
Click to enable flow control for fixed speed settings.
When "*Auto*" Speed is selected for a port, this selection indicates the flow control capability that is advertised to the link partner.

Maximum Frame
Enter the maximum frame size allowed for the switch port, including FCS.
The allowed range is *1518* bytes to *9600* bytes.

Excessive Collision Mode
Configure port transmission collision behavior.
Discard: Discard frame after 16 collisions (default).
Restart: Restart back-off algorithm after 16 collisions.

Power Control
The column allows for changing the power savings mode parameters per port.



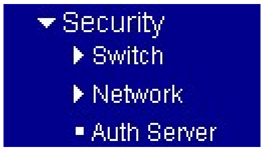
Disabled: All power savings mechanisms are disabled.
ActiPHY: Link down power savings is enabled.
PerfectReach: Link up power savings is enabled.
Enabled: Both link up and link down power savings are enabled.

Save
Click to save the changes.

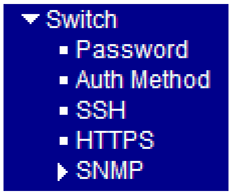
Reset
Click to undo any changes made locally and revert to previously saved values.

Refresh
Click to refresh the page. Any changes made locally will be undone.

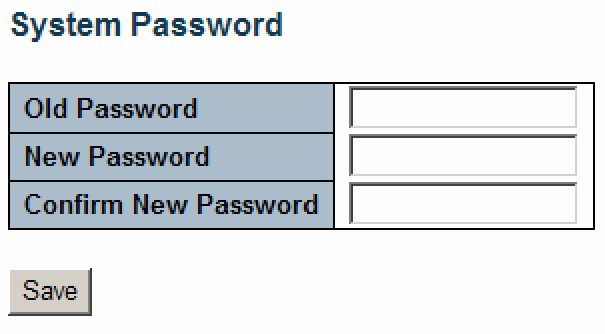
2.3 Security



2.3.1 Switch

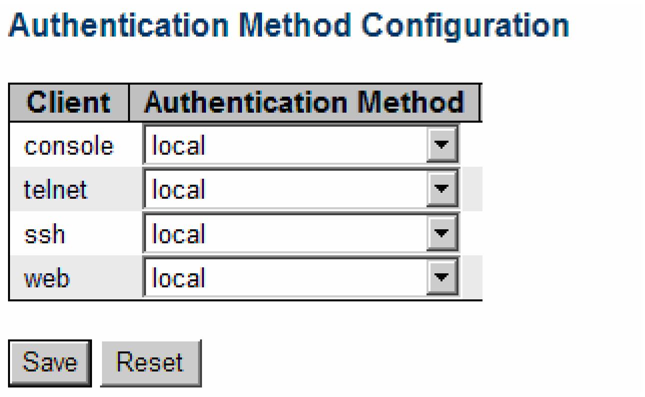


2.3.1.1 Password



Configuration	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	New system password to be used Allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm New Password	Re-enter the new system password.
Save	Click to save the changes.

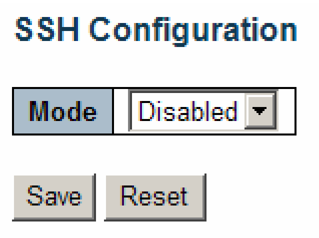
2.3.1.2 Auth Method


Authentication Method Configuration

Client	Authentication Method
console	local
telnet	local
ssh	local
web	local

Configuration	Description
Client	Access method to the switch – telnet, ssh, web, console
Authentication Method	Authentication can be set to one of the following values: ***none:*** authentication is disabled and login is not possible. ***local:*** use the local user database on the switch for authentication. ***RADIUS:*** use a remote RADIUS server for authentication.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

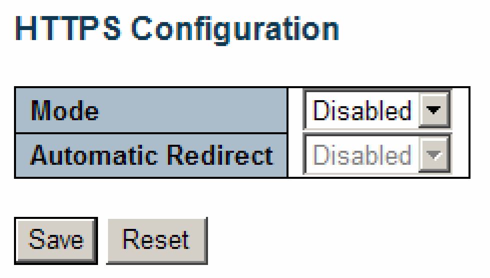
2.3.1.3 SSH



Mode: Disabled

Configuration	Description
Mode	Indicates the SSH mode operation. Possible modes are: ***Enabled:*** Enable SSH mode operation. ***Disabled:*** Disable SSH mode operation.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.1.4 HTTPS

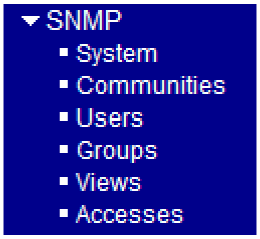


HTTPS Configuration

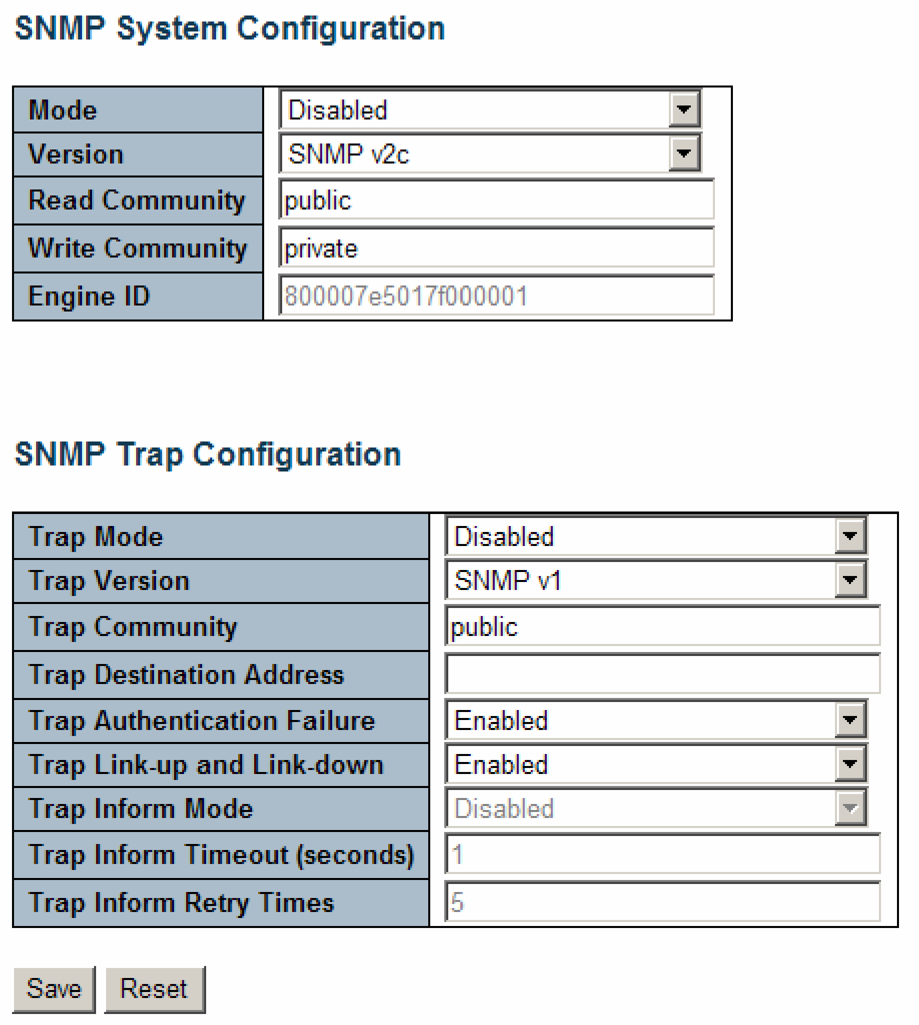
Mode	Disabled
Automatic Redirect	Disabled

Configuration	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: ***Enabled:*** Enable HTTPS mode operation. ***Disabled:*** Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: ***Enabled:*** Enable HTTPS redirect mode operation. ***Disabled:*** Disable HTTPS redirect mode operation.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.1.5 SNMP



2.3.1.5.1 System



SNMP System Configuration

Mode	Disabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

System Configuration	Description
Mode	Indicates the SNMP mode operation. Possible modes are: ***Enabled:*** Enable SNMP mode operation. ***Disabled:*** Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: ***SNMP v1:*** Set SNMP supported version 1.

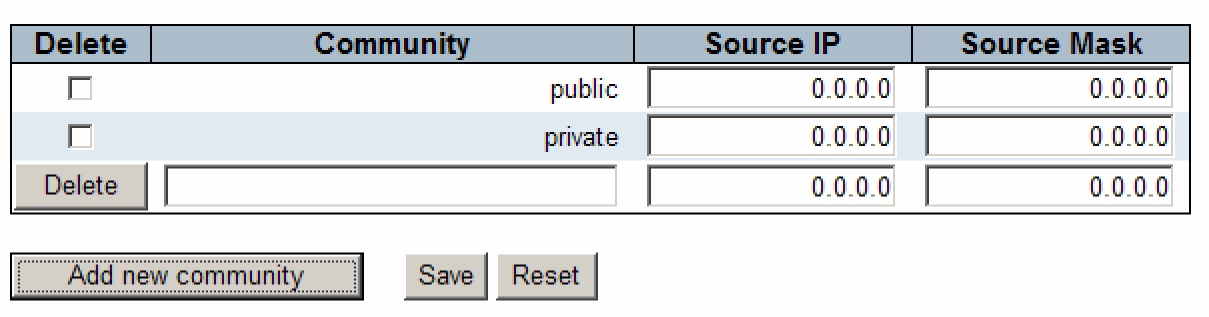
	SNMP v2c: Set SNMP supported version 2c. ***SNMP v3:*** Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is ***0 ~ 255***, and the allowed content is the ASCII characters from 33 to 126. *Note: This field only suits when SNMP version is setting SNMPv1 or SNMPv2c. If SNMP version is setting SNMPv3, the community string will associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can use to restrict source subnet.*
Write Community	Indicates the community write-access string to permit access to SNMP agent. The allowed string length is ***0 ~ 255***, and the allowed content is the ASCII characters from 33 to 126. *Note: This field only suits when SNMP mode version setting SNMPv1 or SNMPv2c. If SNMP version is setting SNMPv3, the community string will associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can use to restrict source subnet.*
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Trap Configuration	**Description**
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap mode operation. ***Disabled:*** Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: ***SNMP v1:*** Set SNMP trap supported version 1. ***SNMP v2c:*** Set SNMP trap supported version 2c. **SNMP v3:** Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is ***0 ~ 255***, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. **Trap Destination IPv6 Address** Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon

	separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: ***Enabled:*** Enable SNMP trap authentication failure. ***Disabled:*** Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap link-up and link-down mode operation. ***Disabled:*** Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: ***Enabled:*** Enable SNMP trap inform mode operation. ***Disabled:*** Disable SNMP trap inform mode operation.
Trap Inform Timeout	Indicates the SNMP trap inform timeout (seconds). The allowed range is ***0 ~ 2147***.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is ***0 ~ 255***.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: ***Enabled:*** Enable SNMP trap probe security engine ID mode of operation. ***Disabled:*** Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

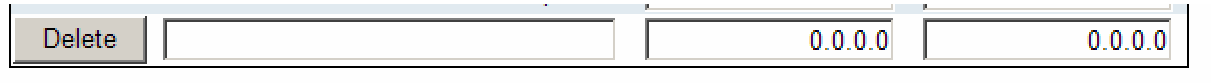
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.1.5.2 Communities



Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0
Delete		0.0.0.0	0.0.0.0

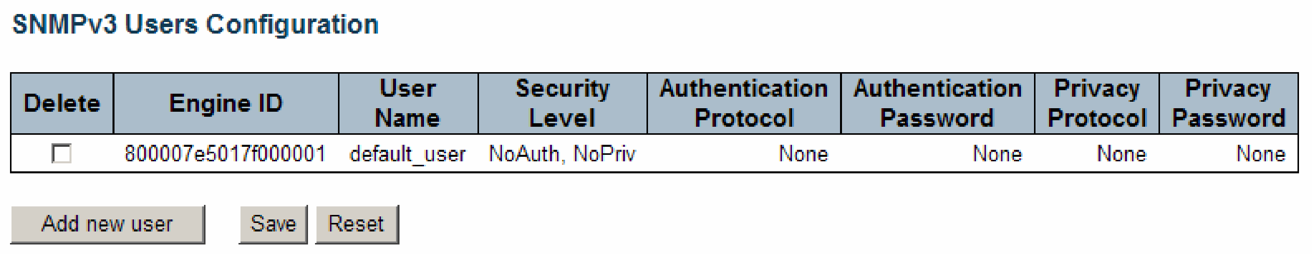
Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. The community string will treat as security name and map a SNMPv1 or SNMPv2c community string.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can use to restrict source subnet when combined with source mask.
Source Mask	Indicates the SNMP access source address mask.
Add new community	Click to add a new community entry as shown below.



Delete		0.0.0.0	0.0.0.0

Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.1.5.3 Users



SNMPv3 Users Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In othe the words, if user engine ID equal system engine ID then it is local user; otherwize it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: ***NoAuth, NoPriv:*** None authentication and none privacy. ***Auth, NoPriv:*** Authentication and none privacy. ***Auth, Priv:*** Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: ***None:*** None authentication protocol. ***MD5:*** An optional flag to indicate that this user using MD5 authentication protocol. ***SHA:*** An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol,

the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.

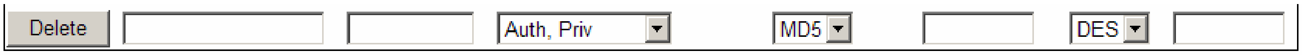
Privacy Protocol
Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: None privacy protocol.

DES: An optional flag to indicate that this user using DES authentication protocol.

Privacy Password
A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Add new user
Click to add a new SNMPv3 user entry as shown below.

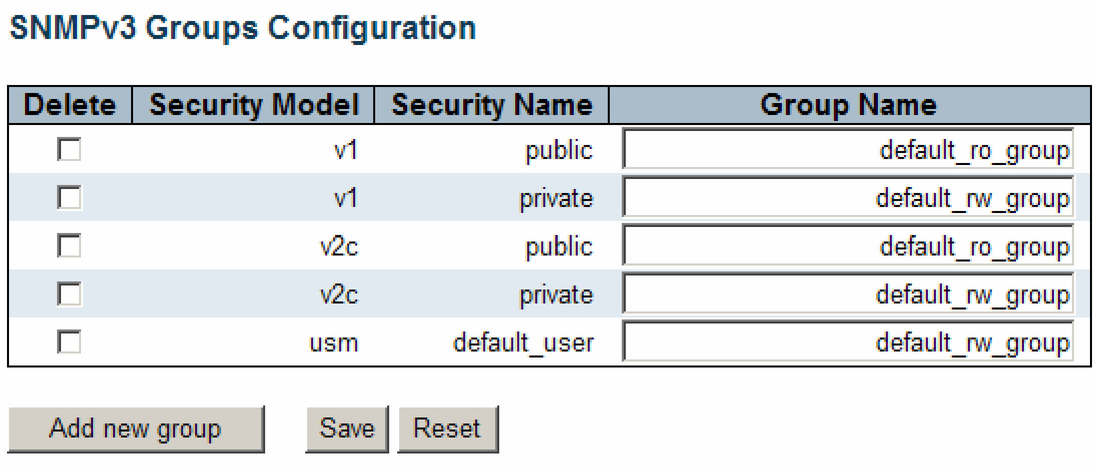


Delete
Click to cancel the new entry.

Save
Click to save the changes.

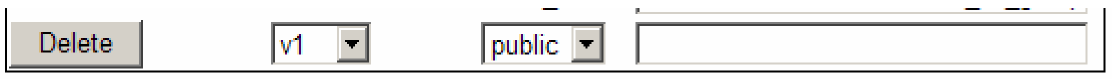
Reset
Click to undo any changes made locally and revert to previously saved values.

2.3.1.5.4 Groups

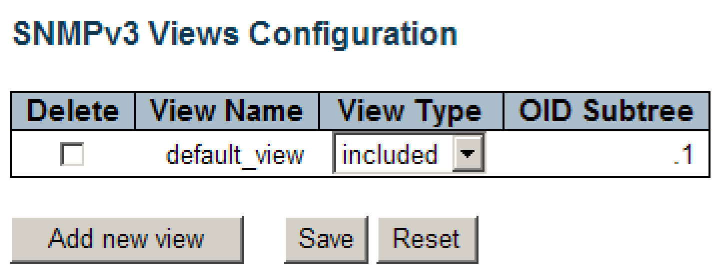


SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

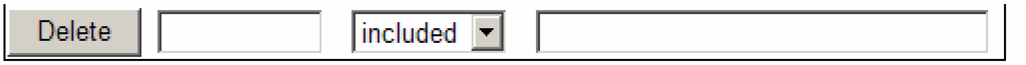
Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: ***v1:*** Reserved for SNMPv1. ***v2c:*** Reserved for SNMPv2c. ***usm:*** User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Add new group	Click to add a new SNMPv3 group entry as shown below.  Delete v1 ▼ public ▼
Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.1.5.5 Views

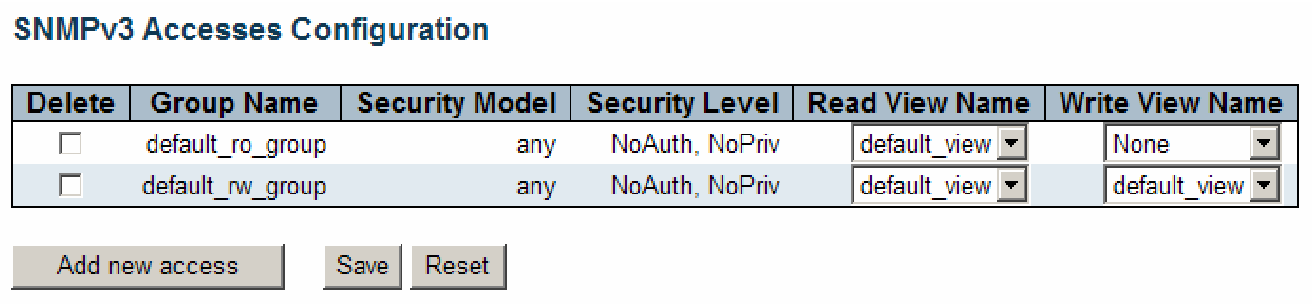


SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included ▾	.1

Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: ***included:*** An optional flag to indicate that this view sub-tree should be included. ***excluded:*** An optional flag to indicate that this view sub-tree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID sub-tree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the sub-tree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).
Add new view	Click to add a new SNMPv3 view entry as shown below. 
Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

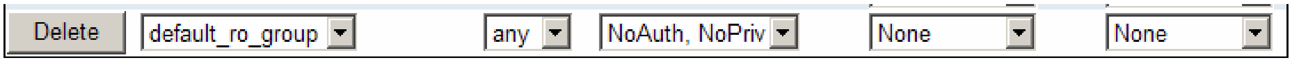
2.3.1.5.6 Accesses



SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view ▾	None ▾
□	default_rw_group	any	NoAuth, NoPriv	default_view ▾	default_view ▾

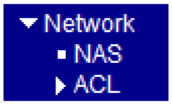
Configuration	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: ***any:*** Accepted any security model (v1|v2c|usm). ***v1:*** Reserved for SNMPv1. ***v2c:*** Reserved for SNMPv2c. ***usm:*** User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: ***NoAuth, NoPriv:*** None authentication and none privacy. ***Auth, NoPriv:*** Authentication and none privacy. ***Auth, Priv:*** Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Add new access	Click to add a new SNMPv3 view entry as shown below.



Delete	default_ro_group ▾	any ▾	NoAuth, NoPriv ▾	None ▾	None ▾

Delete	Click to cancel the new entry.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

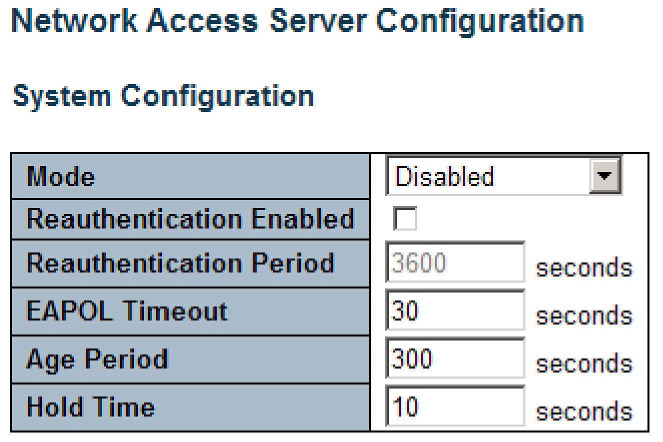
2.3.2 Network



2.3.2.1 NAS

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

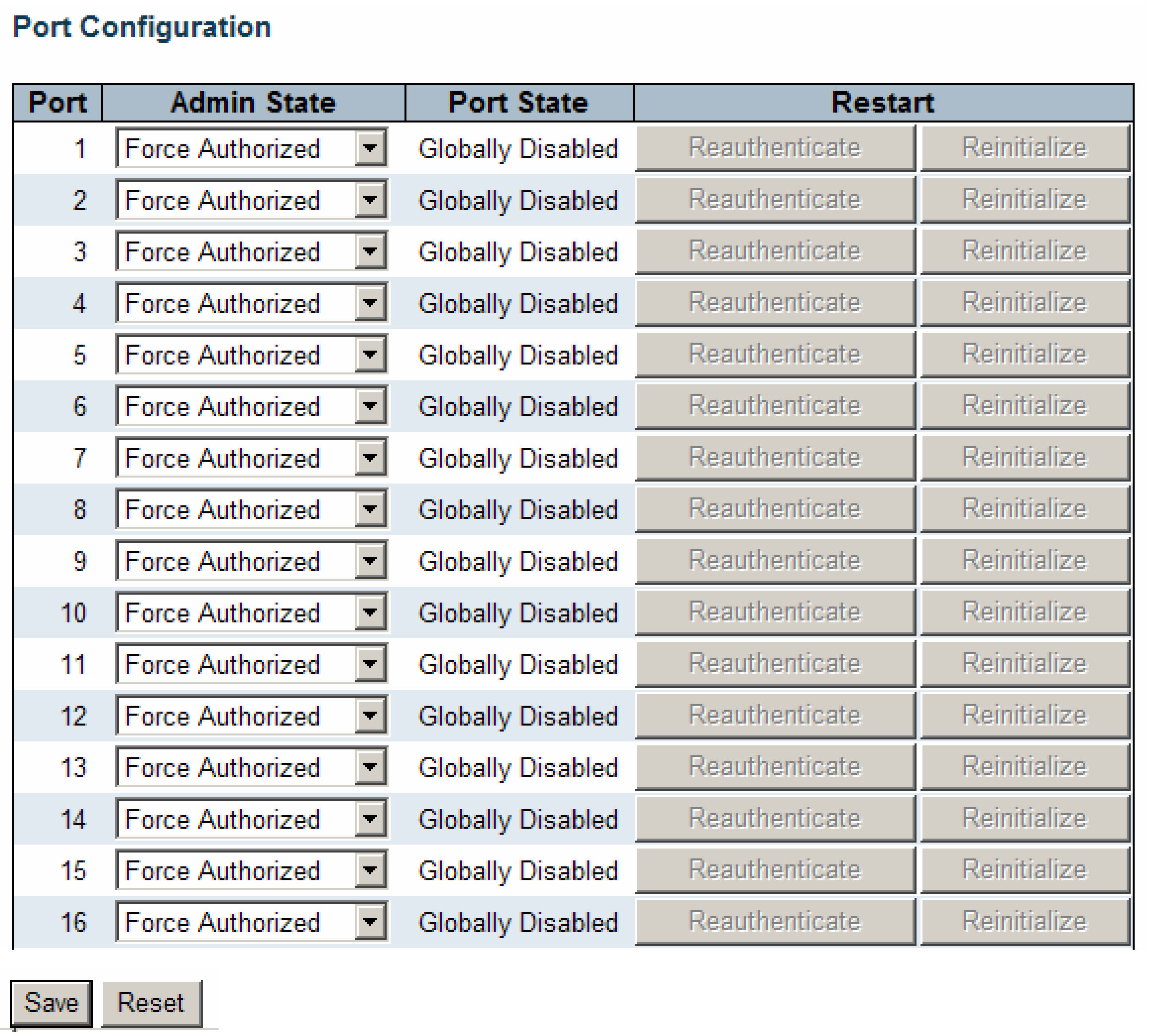
MAC-based authentication allows for authentication of more than one user on the same port, and doesn’t require the user to have special 802.1X software installed on his system. The switch uses the user’s MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than the 802.1X authentication.



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds



Port Configuration

Port	Admin State	Port State	Restart	
1	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

System Configuration	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch unit. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	If checked, clients are re-authenticated after the interval specified by the Reauthentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn’t imply that a client is still present on a port (see Age Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values: ***1 ~ 3600** seconds*

EAPOL Timeout

Determines the time the switch shall wait for the supplicant response before retransmitting a packet.

Valid values: ***1 ~ 255** seconds (This has no effect for MAC-based ports.)*

Age Period

This setting applies to ports running *MAC-based authentication,* only.

Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Re-authentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between *10* and *1000000* seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 for him to stay authenticated.

Hold Time

This setting applies to ports running *MAC-based authentication,* only.

If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication configuration page), the client is put on hold in the "*Unauthorized*" state. In this state, frames from the client will not cause the switch to attempt to re-authenticate the client. The Hold Time, which can be set to a number between ***10 ~ 1000000*** seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access.

Port Configuration **Description**

Port

The port number for which the configuration below applies.

Admin State

Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled):

Auto: Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.

Authorized: Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up.

Unauthorized: Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up.

MAC-Based: Enables MAC-based authentication on the port. The switch doesn’t transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.

Port State

The current state of the port. It can undertake one of the following values:

Disabled: 802.1X and MAC-based authentication is globally disabled.

Link Down: 802.1X or MAC-based authentication is enabled, but there is no link on the port.

Authorized: The port is authorized. This is the case when 802.1X Authentication is enabled, the port has link, and the Admin State is “Auto” and the supplicant is authenticated or the Admin State is “Authorized”.

Unauthorized: The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is “Auto”, but the supplicant is not (yet) authenticated or the Admin State is “Unauthorized”.

X Auth/Y Unauth: X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to “MAC-Based”.

Restart

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port’s Admin State is “*Auto*” or “*MAC-Based*”.

Clicking these buttons will not cause settings changed on the page to take effect.

Reauthenticate: Schedules a re-authentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, re-authentication will be attempted immediately.

The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized.

Reinitialize: Forces a re-initialization of the port/clients and thereby a re-authentication immediately. The port/clients will transfer to the unauthorized state while the re-authentication is ongoing.

Save — Click to save the changes.

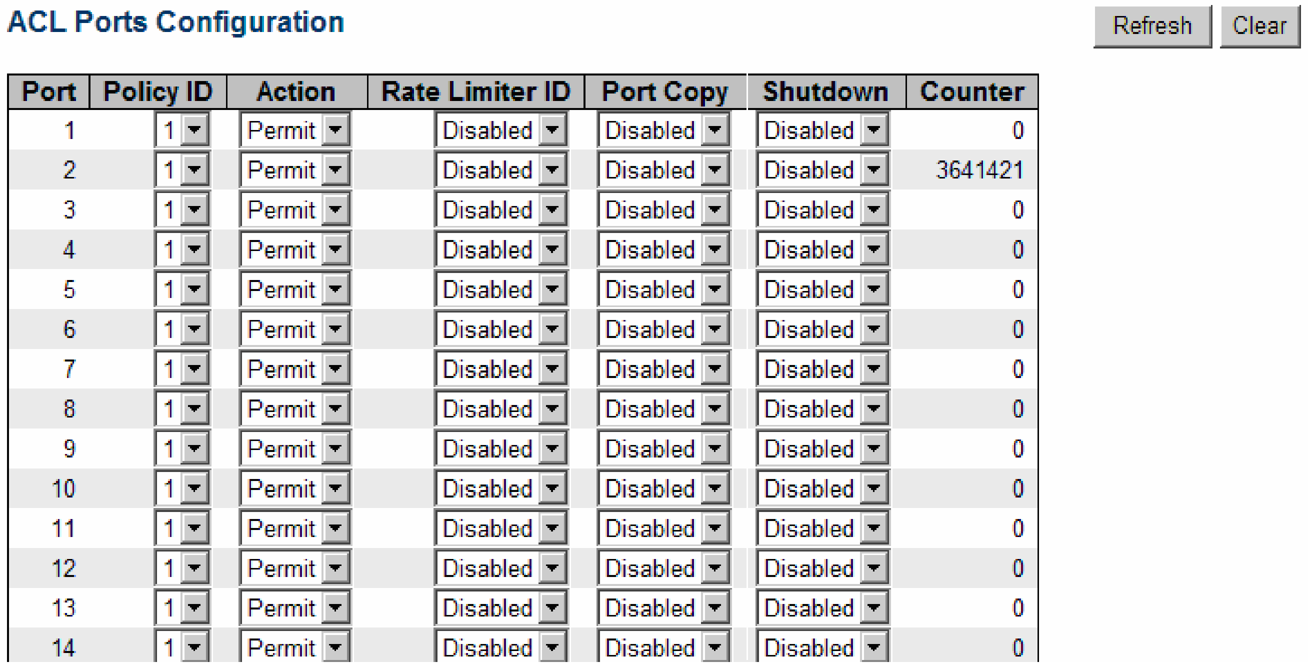
Reset — Click to undo any changes made locally and revert to previously saved values.

Refresh — Click to refresh the page. Any changes made locally will be undone.

2.3.2.2 ACL

2.3.2.2.1 Ports

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



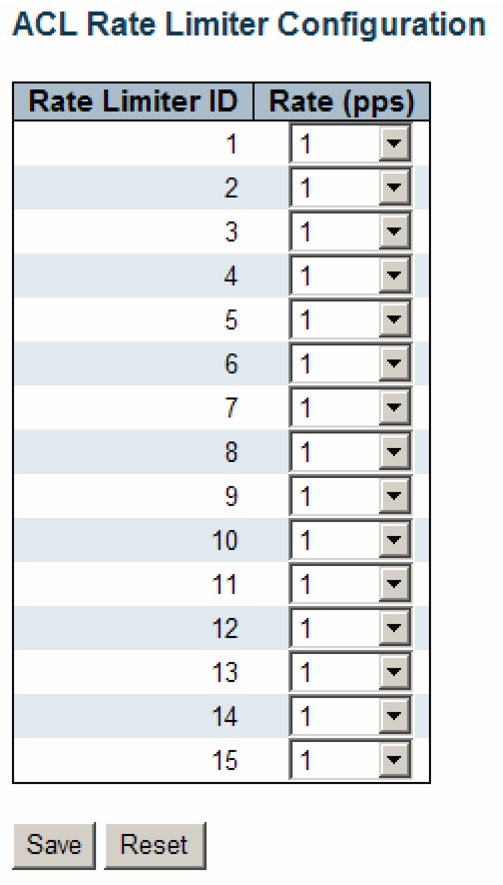
ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	3641421
3	1	Permit	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	Disabled	0

Configuration	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are ***1 ~ 8***. The default value is 1.
Action	Select whether forwarding is permitted ("***Permit***") or denied ("***Deny***"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are ***Disabled*** or the values ***1 ~ 15***. The default value is "***Disabled***".
Port Copy	Select which port frames are copied to. The allowed values are ***Disabled*** or a specific port number. The default value is "***Disabled***".
Shutdown	Specify the port shut down operation of this port. The allowed values are: ***Enabled:*** If a frame is received on the port, the port will be disabled.

	Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear the counters.

2.3.2.2.2 Rate Limiters

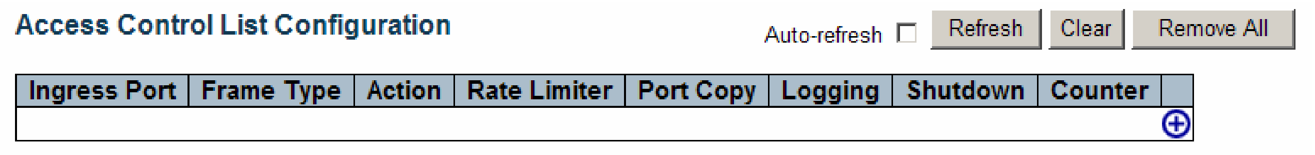


ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

Configuration	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as ***1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K,*** or ***1024K***. The 1 kpps is actually 1002.1 pps.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.2.2.3 Access Control Lists



Access Control List Configuration

Auto-refresh □ Refresh Clear Remove All

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
								⊕

Configuration	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: ***Any:*** The ACE will match any ingress port. ***Policy:*** The ACE will match ingress ports with a specific policy. ***Port:*** The ACE will match a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are: ***Any:*** The ACE will match any frame type. ***EType:*** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ***ARP:*** The ACE will match ARP/RARP frames. ***IPv4:*** The ACE will match all IPv4 frames. ***IPv4/ICMP:*** The ACE will match IPv4 frames with ICMP protocol. ***IPv4/UDP:*** The ACE will match IPv4 frames with UDP protocol. ***IPv4/TCP:*** The ACE will match IPv4 frames with TCP protocol. ***IPv4/Other:*** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
Action	Indicates the forwarding action of the ACE. ***Permit:*** Frames matching the ACE may be forwarded and learned. ***Deny:*** Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is ***1 ~ 15***. When "***Disabled***" is displayed, the rate limiter operation is disabled.
Port Copy	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are ***Disabled*** or a ***specific port number***. When Disabled is displayed, the port copy operation is disabled.
Logging	Indicates the logging operation of the ACE. Possible values are: ***Enabled:*** Frames matching the ACE are stored in the System Log. ***Disabled:*** Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Indicates the port shut down operation of the ACE. Possible values are: ***Enabled:*** If a frame matches the ACE, the ingress port will be disabled. ***Disabled:*** Port shut down is disabled for the ACE.

Counter The counter indicates the number of times the ACE was hit by a frame.

Auto-refresh Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

ACE modification buttons:

(+) Inserts a new ACE before the current row.

(e) Edits the ACE.

(↑) Moves the ACE up the list.

(↓) Moves the ACE down the list.

(X) Deletes the ACE.

(+) The lowest plus sign adds a new entry at the bottom of the list of ACL.

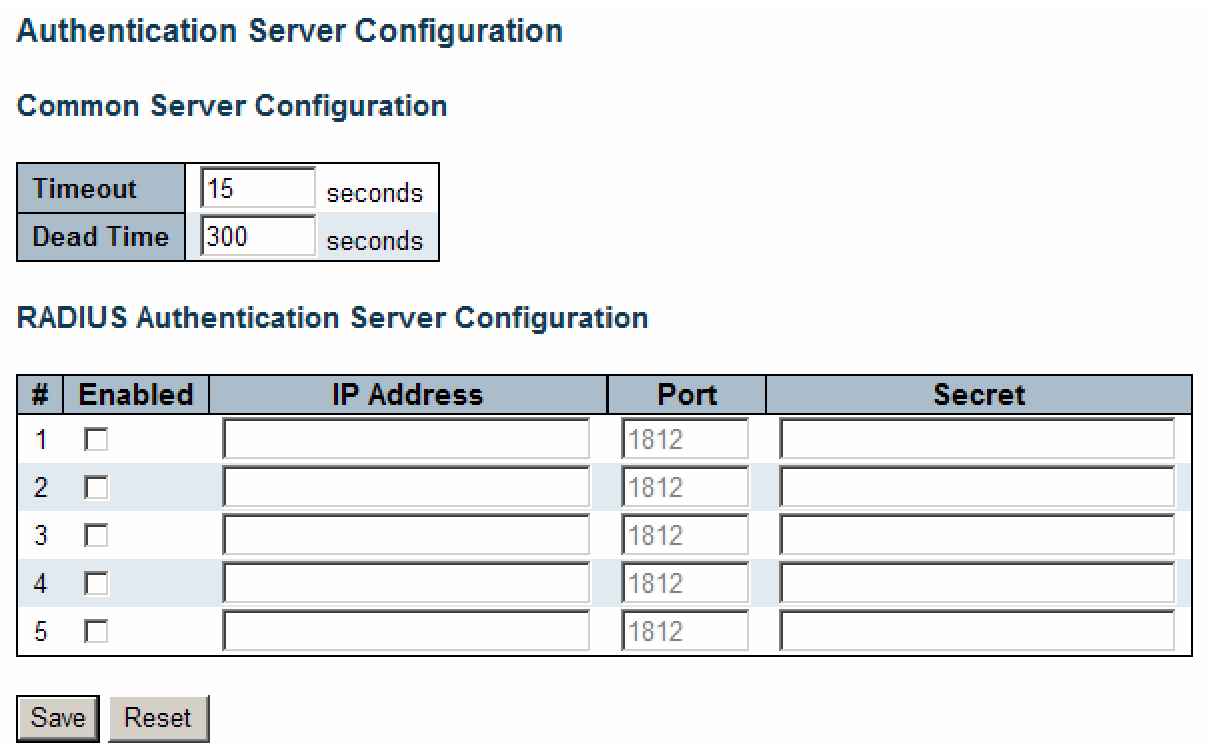
Refresh Click to refresh the page; any changes made locally will be undone.

Clear Click to clear the counters.

Remove All Click to remove all ACEs.

Remark: The maximum number of ACEs is 128.

2.3.3 Auth Server



Authentication Server Configuration

Common Server Configuration

Timeout	15 seconds
Dead Time	300 seconds

RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	□		1812	
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

Common Server	Description
Timeout	The Timeout, which can be set to a number between *3* and *3600* seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between *0* and *3600* seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration	
#	The RADIUS authentication server number for which the configuration applies

Enabled	Enable the RADIUS Authentication Server by checking this box.
IP Address	The IP address of the RADIUS Authentication Server expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to zero (0), the default port (1812) is used for the RADIUS Authentication Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch unit.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.4 Aggregation

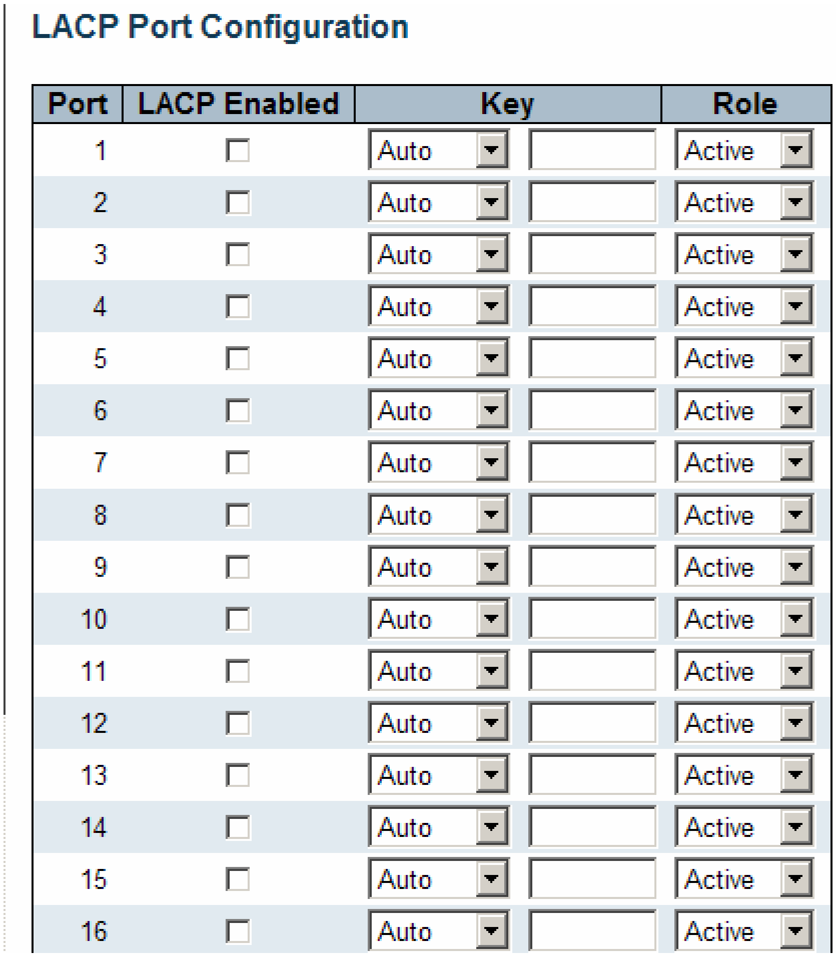
The Port Link Aggregation function can combine multiple physical switched ports, called “Aggregation Group” into one logical port. It allows making connection between two switches using more than one physical links to increase the connection bandwidth between two switches.

Note:

Maximum number of aggregation groups in one 24-Port switch: 12

Maximum number of physical switched port members per group: no limit

2.4.1 LACP



LACP Port Configuration

Port	LACP Enabled	Key		Role
1	□	Auto		Active
2	□	Auto		Active
3	□	Auto		Active
4	□	Auto		Active
5	□	Auto		Active
6	□	Auto		Active
7	□	Auto		Active
8	□	Auto		Active
9	□	Auto		Active
10	□	Auto		Active
11	□	Auto		Active
12	□	Auto		Active
13	□	Auto		Active
14	□	Auto		Active
15	□	Auto		Active
16	□	Auto		Active

Configuration	Description
Port	The port number for which the associated row configuration applies
LACP Enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
Key	The Key value incurred by the port, range ***1- 65535***.

Auto: set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3.

Specific: a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role — The Role shows the LACP activity status. The "***Active***" will transmit LACP packets each second while "***Passive***" will wait for a LACP packet from a link partner (speak if spoken to).

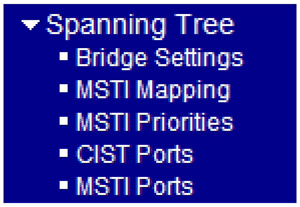
Save — Click to save the changes.

Reset — Click to undo any changes made locally and revert to previously saved values.

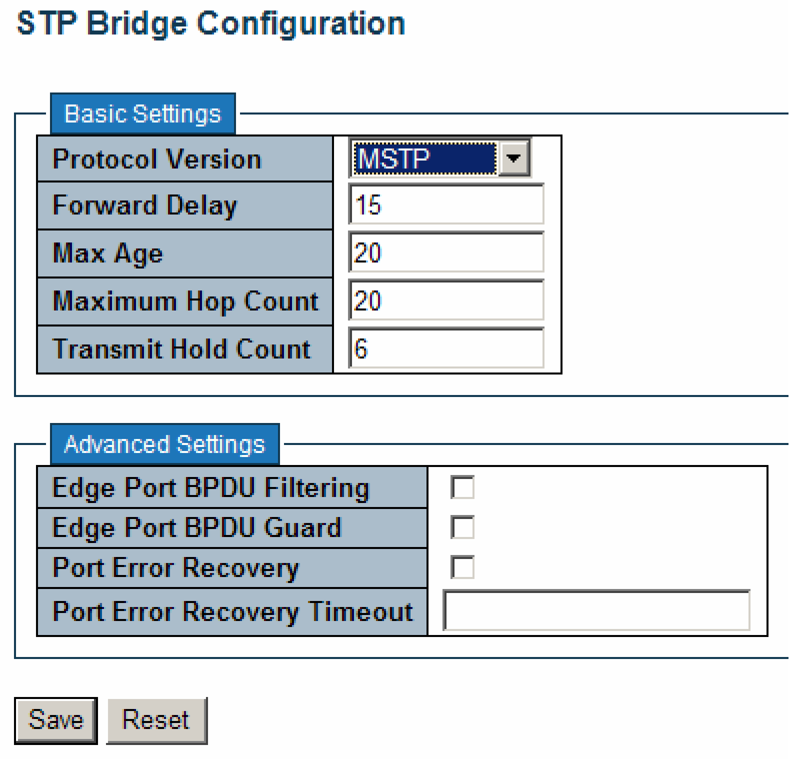
Note: LLAG means LACP Link Aggregation Groups.

2.5 Spanning Tree

This section is used to set configuration for supporting Spanning Tree protocols including STP, RSTP, and MSTP.



2.5.1 Bridge Settings



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Basic Configuration	Description
Protocol Version	The STP protocol version setting Valid values: ***STP, RSTP, MSTP***
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values: ***4 ~ 30 seconds***
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge Valid values: ***6 ~ 40 seconds*** *(Max Age must be <= (FwdDelay-1)*2)*
Maximum Hop Count	It defines how many bridges a root bridge can distribute its BPDU information. This

defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region.

Transmit Hold Count

The number of BPDU’s a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed.
Valid values: ***1 ~ 10*** *BPDU’s per second*

Advanced Configuration

Edge Port BPDU Filtering

Check to configure a port *explicitly* as *Edge* will transmit and receive BPDUs

Edge Port BPDU Guard

Control whether a port *explicitly* configured as *Edge* will disable itself upon reception of a BPDU. The port will enter the *error-disabled* state, and will be removed from the active topology.

Port Error Recovery

Control whether a port in the *error-disabled* state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout

The time that has to pass before a port in the *error-disabled* state can be enabled.
Valid values: ***30 ~ 86400*** *seconds (24 hours)*

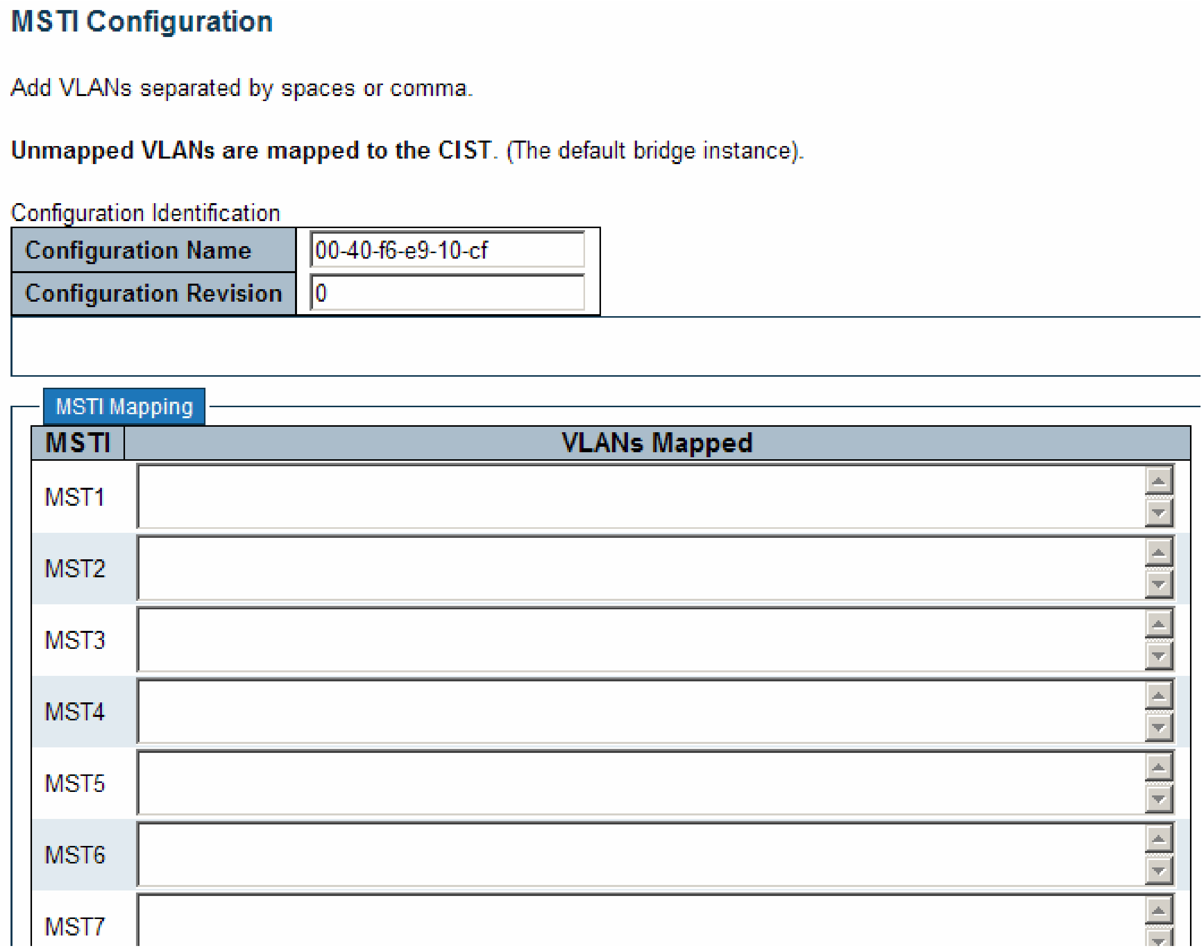
Save

Click to save the changes.

Reset

Click to undo any changes made locally and revert to previously saved values.

2.5.2 MSTI Mapping



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-40-f6-e9-10-cf
Configuration Revision	0

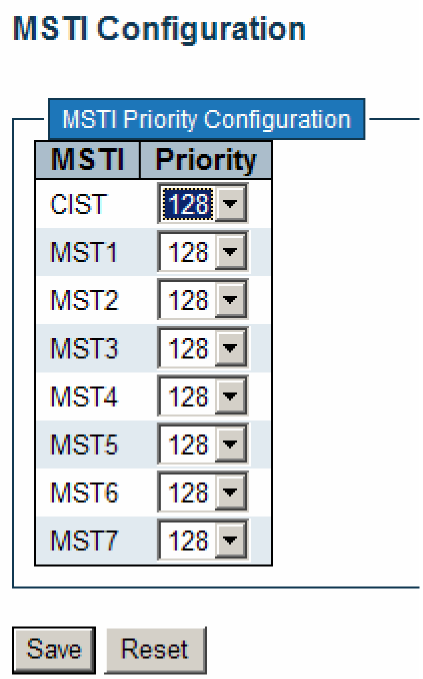
MSTI Mapping

MSTI	VLANs Mapped
MST1	
MST2	
MST3	
MST4	
MST5	
MST6	
MST7	

Configuration	Description
Configuration Name	The name identifying the VLAN to MSTI mapping Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region) The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between ***0 ~ 65535***.
MSTI Mapping	
MSTI	The bridge instance The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (i.e. not having any VLANs mapped to it.)

Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.3 MSTI Priorities



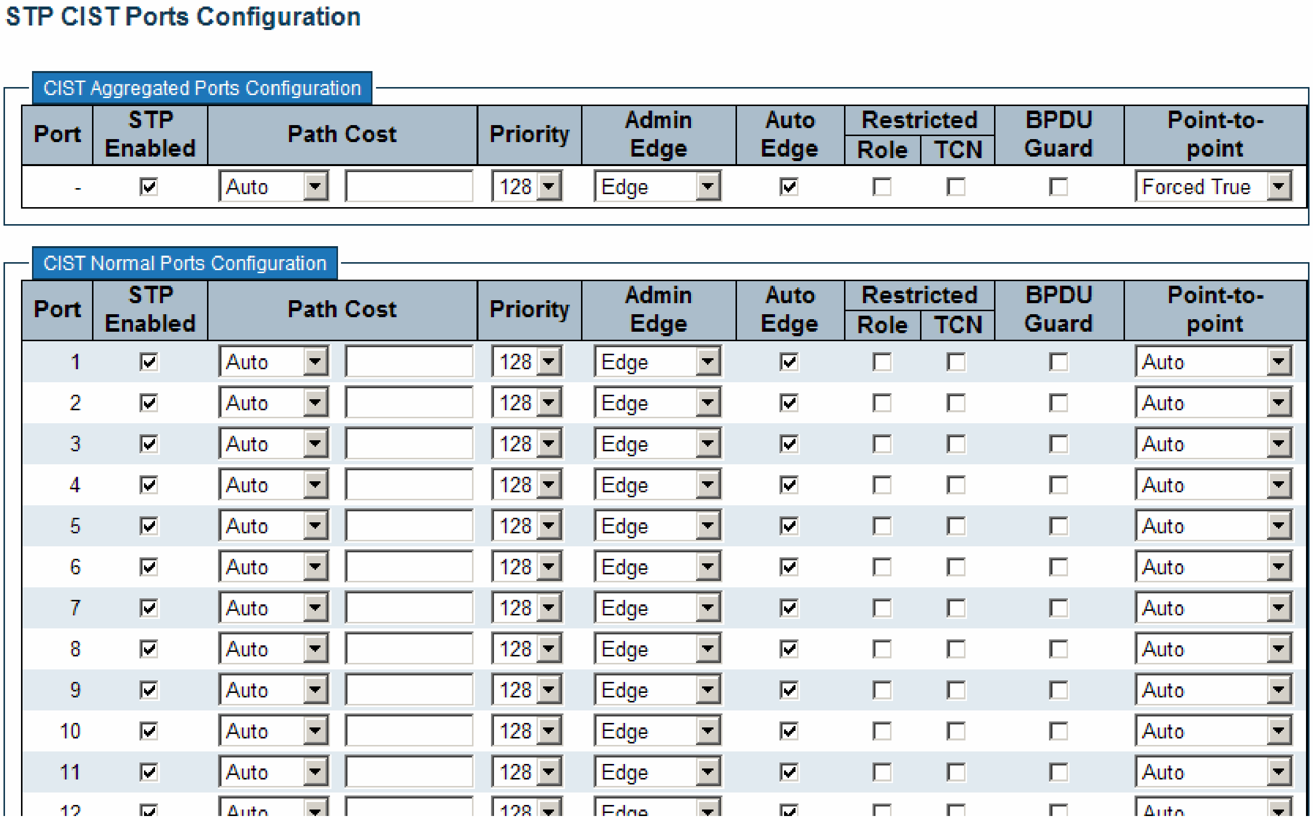
MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
CIST	128
MST1	128
MST2	128
MST3	128
MST4	128
MST5	128
MST6	128
MST7	128

Configuration	Description
MSTI	The bridge instance. The CIST is the *default* instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.5.4 CIST Ports



STP CIST Ports Configuration

CIST Aggregated Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Edge	☑	□	□	□	Forced True

CIST Normal Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
1	☑	Auto		128	Edge	☑	□	□	□	Auto
2	☑	Auto		128	Edge	☑	□	□	□	Auto
3	☑	Auto		128	Edge	☑	□	□	□	Auto
4	☑	Auto		128	Edge	☑	□	□	□	Auto
5	☑	Auto		128	Edge	☑	□	□	□	Auto
6	☑	Auto		128	Edge	☑	□	□	□	Auto
7	☑	Auto		128	Edge	☑	□	□	□	Auto
8	☑	Auto		128	Edge	☑	□	□	□	Auto
9	☑	Auto		128	Edge	☑	□	□	□	Auto
10	☑	Auto		128	Edge	☑	□	□	□	Auto
11	☑	Auto		128	Edge	☑	□	□	□	Auto
12	☑	Auto		128	Edge	☑	□	□	□	Auto

Configuration	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The ***Auto*** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the ***Specific*** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values: ***1 to 200000000***
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
AdminEdge	Controls whether the *operEdge* flag should start as being set or cleared. (The initial *operEdge* state when a port is initialized). *operEdge: Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having* operEdge *true) than for other ports.*
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge

port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not.

Restricted-Role
If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.
This feature is also know as ***Root Guard***.

Restricted TCN
If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.

BPDU Guard
If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port *Edge* status does not affect this setting.
A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point2Point
Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Save
Click to save the changes.

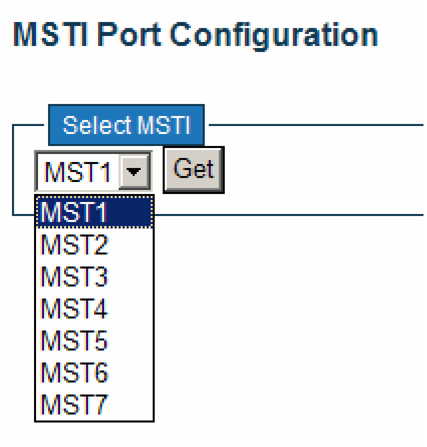
Reset
Click to undo any changes made locally and revert to previously saved values.

Note: This configuration applies to physical and Link Aggregation ports.

2.5.5 MSTI Ports

A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.

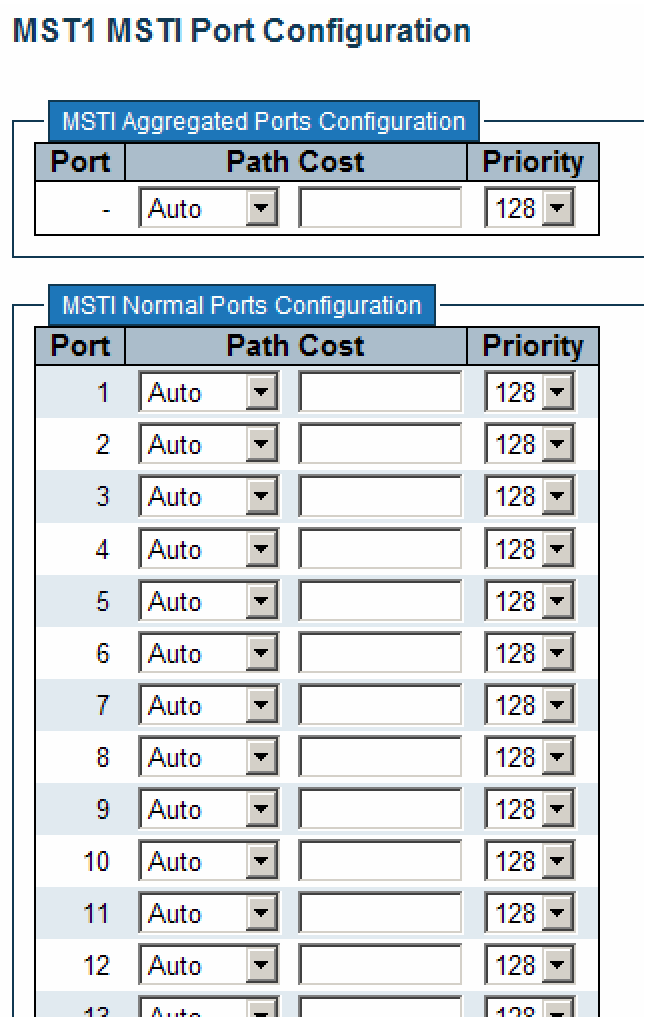


MSTI Port Configuration

Select MSTI

MST1 ▾ Get

Configuration	Description
MSTI	Select an MSTI for pop-up configuration.
Get	Click to pop-up configuration page.



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

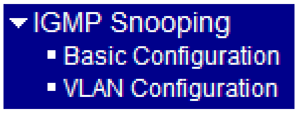
Port	Path Cost		Priority
-	Auto ▾		128 ▾

MSTI Normal Ports Configuration

Port	Path Cost		Priority
1	Auto ▾		128 ▾
2	Auto ▾		128 ▾
3	Auto ▾		128 ▾
4	Auto ▾		128 ▾
5	Auto ▾		128 ▾
6	Auto ▾		128 ▾
7	Auto ▾		128 ▾
8	Auto ▾		128 ▾
9	Auto ▾		128 ▾
10	Auto ▾		128 ▾
11	Auto ▾		128 ▾
12	Auto ▾		128 ▾
13	Auto ▾		128 ▾

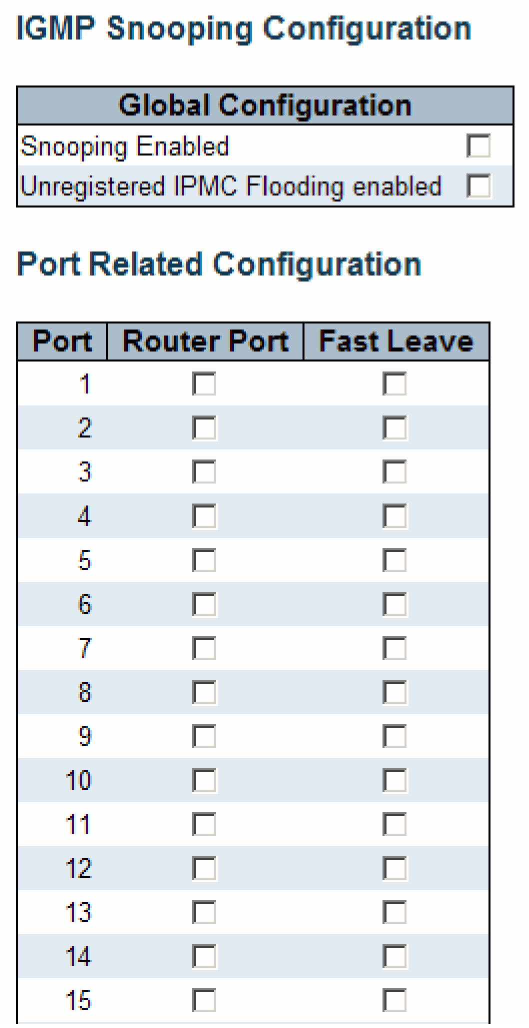
Configuration	Description (Example with MSTI1)
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The ***Auto*** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the ***Specific*** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values: ***1 ~ 200000000***
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.6 IGMP Snooping



- IGMP Snooping
  - Basic Configuration
  - VLAN Configuration

2.6.1 Basic Configuration



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMC Flooding enabled	□

Port Related Configuration

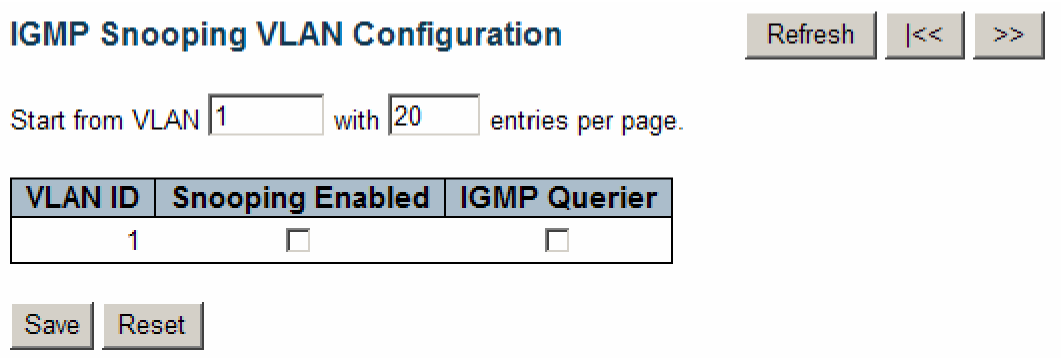
Port	Router Port	Fast Leave
1	□	□
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□
7	□	□
8	□	□
9	□	□
10	□	□
11	□	□
12	□	□
13	□	□
14	□	□
15	□	□

Global Configuration	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC	Flooding enabled
	Enable unregistered IPMC traffic flooding.

Port Configuration	Description
Port	The port number for which the row configuration applies

Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.6.2 VLAN Configuration



IGMP Snooping VLAN Configuration

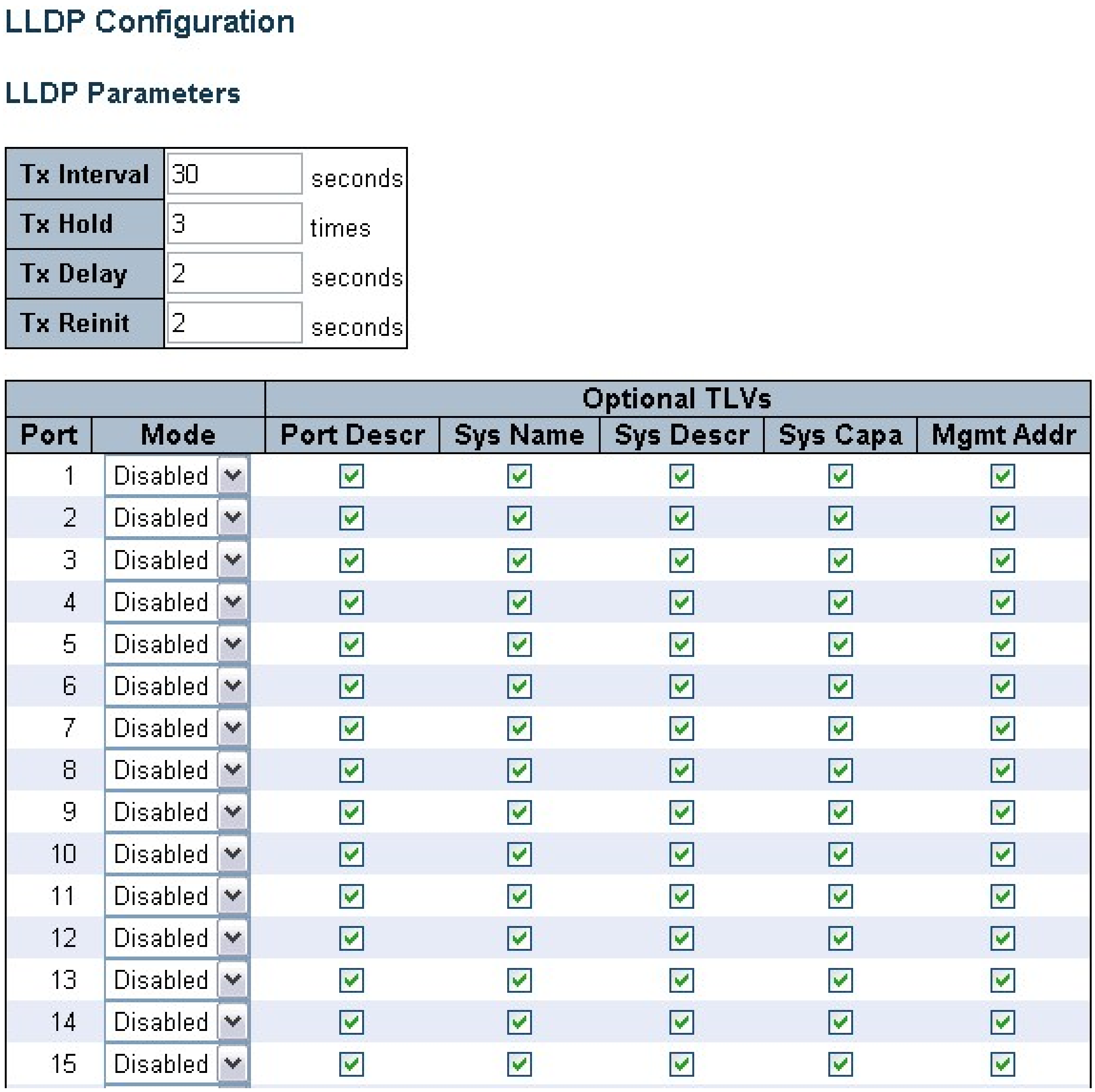
Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	IGMP Querier
1	□	□

VLAN Configuration	Description
Start from VLAN …..	Select range of VLAN table entries.
VLAN ID	The VLAN ID of the entry.
Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.
Refresh	Click to refresh the page; any changes made locally will be undone.
|<<	Click to display the first page.
>>|	Click to display the last page.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.7 LLDP

2.7.1 LLDP



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	3	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

		Optional TLVs				
Port	**Mode**	**Port Descr**	**Sys Name**	**Sys Descr**	**Sys Capa**	**Mgmt Addr**
1	Disabled	☑	☑	☑	☑	☑
2	Disabled	☑	☑	☑	☑	☑
3	Disabled	☑	☑	☑	☑	☑
4	Disabled	☑	☑	☑	☑	☑
5	Disabled	☑	☑	☑	☑	☑
6	Disabled	☑	☑	☑	☑	☑
7	Disabled	☑	☑	☑	☑	☑
8	Disabled	☑	☑	☑	☑	☑
9	Disabled	☑	☑	☑	☑	☑
10	Disabled	☑	☑	☑	☑	☑
11	Disabled	☑	☑	☑	☑	☑
12	Disabled	☑	☑	☑	☑	☑
13	Disabled	☑	☑	☑	☑	☑
14	Disabled	☑	☑	☑	☑	☑
15	Disabled	☑	☑	☑	☑	☑

Global Configuration	**Description**
Tx Interval	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values: ***5 – 32768** seconds*
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold**

multiplied by **Tx Interval** seconds.

Valid values: ***2 – 10 times***

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value.

Valid values: ***1 – 8192 seconds***

Tx Reinit

When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization.

Valid values: ***1 – 10 seconds***

Port Configuration

Port

The switch port number of the logical LLDP port.

Mode

Select LLDP mode.

Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

Optional TLV

Port Descr

When checked the "port description" is included in LLDP information transmitted.

Sys Name

When checked the "system name" is included in LLDP information transmitted.

Sys Descr

When checked the "system description" is included in LLDP information transmitted.

Sys Capa

When checked the "system capability" is included in LLDP information transmitted.

Mgmt Addr

When checked the "management address" is included in LLDP information transmitted.

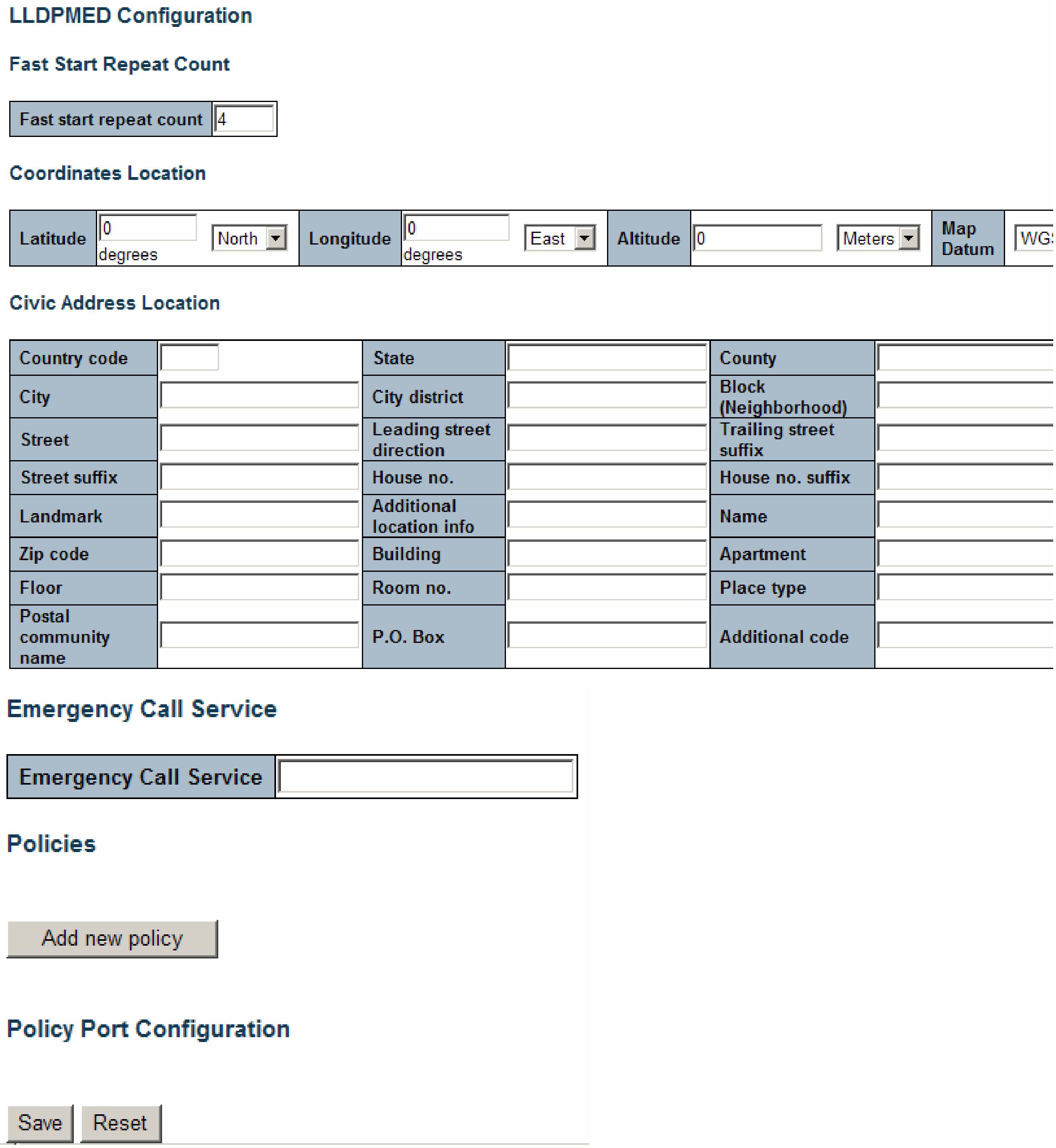
Save

Click to save the changes.

Reset

Click to undo any changes made locally and revert to previously saved values.

2.7.2 LLDP-MED



LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Coordinates Location

Latitude	0 degrees	North	Longitude	0 degrees	East	Altitude	0	Meters	Map Datum	WG

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Policy Port Configuration

Configuration	Description
Fast start repeat count	The number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received.

Coordinates Location

Latitude	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either *North* of the equator or *South* of the equator.
Longitude	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either *East* of the prime meridian or *West* of the prime meridian.
Altitude	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). *Meters*: Representing meters of Altitude defined by the vertical datum specified. *Floors*: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The Map Datum used for the coordinates given in this Option ***WGS84***: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. ***NAD83/NAVD88***: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). ***NAD83/MLLW***: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
Civic Address Location	
Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen
City district	City division, borough, city district, ward, chou (Japan)
Block (Neighborhood)	Neighborhood, block
Street	Street - Example: Poppelvej
Leading street direction	Leading street direction - Example: N
Trailing street suffix	Trailing street suffix - Example: SW

Street suffix	Street suffix - Example: Ave, Platz
House no.	House number - Example: 21
House no. suffix	House number suffix - Example: A, 1/2
Landmark	Landmark or vanity address - Example: Columbia University
Additional location info	Additional location info - Example: South Wing
Name	Name (residence and office occupant) - Example: Flemming Jahn
Zip code	Postal/zip code - Example: 2791
Building	Building (structure) - Example: Low Library
Apartment	Unit (Apartment, suite) - Example: Apt 42
Floor	Floor - Example: 4
Room no.	Room number - Example: 450F
Place type	Place type - Example: Office
Postal community name	Postal community name - Example: Leonia
P.O. Box	Post office box (P.O. BOX) - Example: 12345
Additional code	Additional code - Example: 1320300003

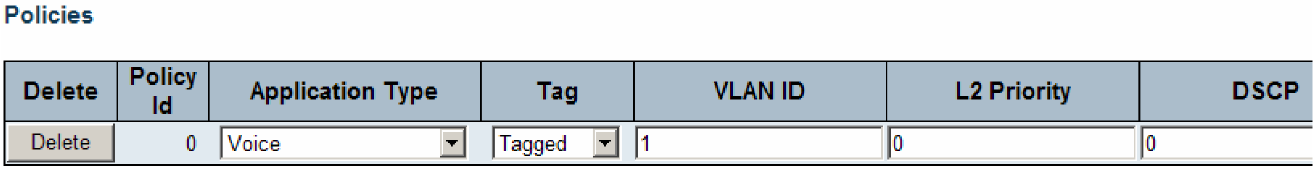
Emergency Call Service

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Add New Policy

Click to configure a new policy.



Policies

Delete	Policy Id	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Delete

Check to delete the policy. It will be deleted during the next save.

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

Application Type

Intended use of the application types:

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. **Voice Signaling** (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type

should not be advertised if all the same network policies apply as those advertised in the **Voice** application policy.

3. **Guest Voice -** support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. **Guest Voice Signaling** (conditional) **-** for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy.

5. **Softphone Voice -** for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

6. **Video Conferencing**

7. **Streaming** Video **-** for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. **Video Signaling** (conditional) **-** for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the **Video Conferencing** application policy.

Tag

Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003

L2 Priority

L2 Priority is the Layer 2 priority to be used for the specified application type. **L2**

	Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP	**DSCP** value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
Port Policies Configuration	
Port	The port number for which the configuration applies.
Policy Id	The set of policies that shall apply for a given port. The set of policies is selected by checkmarking the checkboxes that corresponds to the policies
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time’ network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice

3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

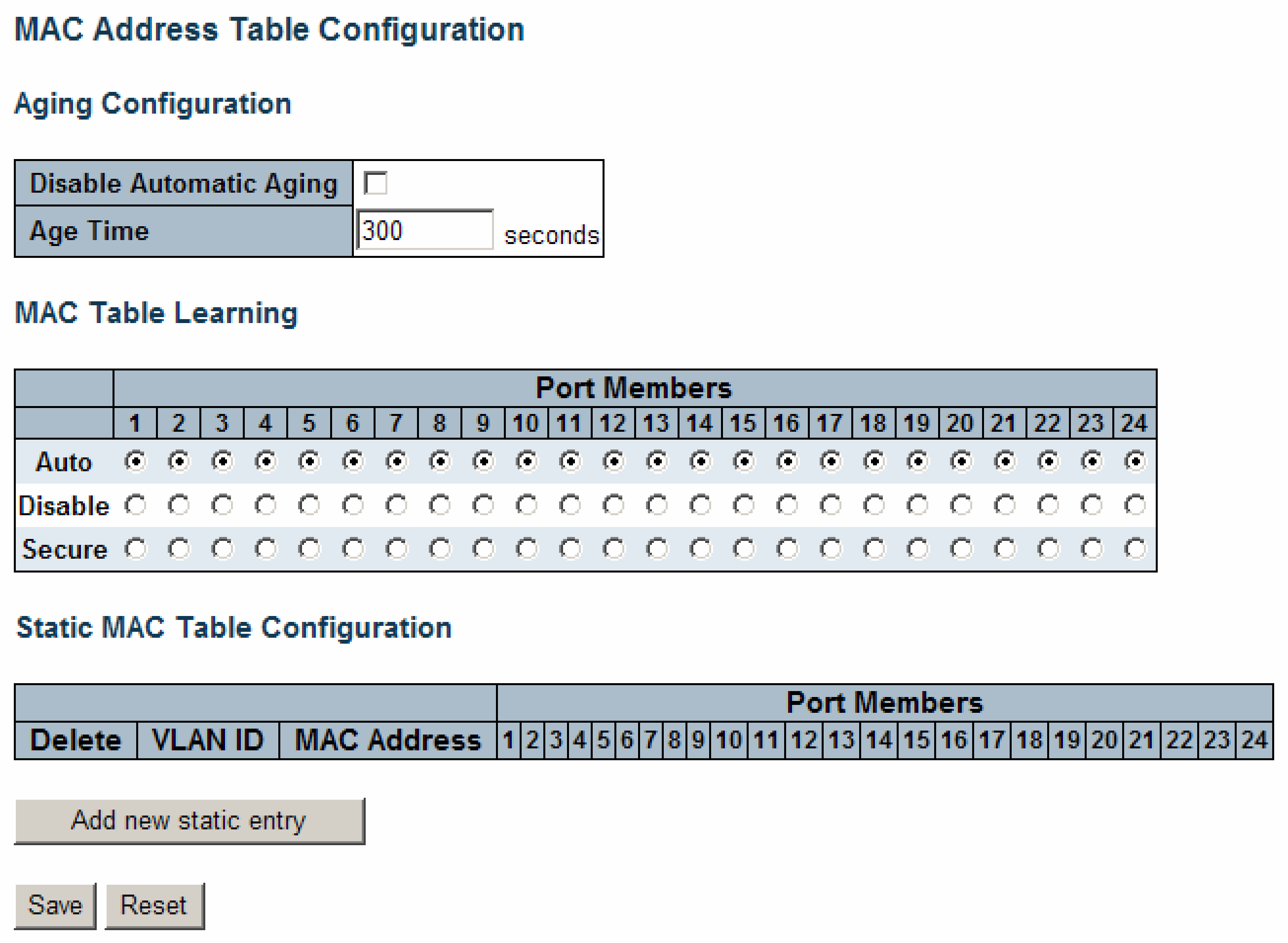
A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

2.8 MAC Table



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Age Time	300 seconds

MAC Table Learning

	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

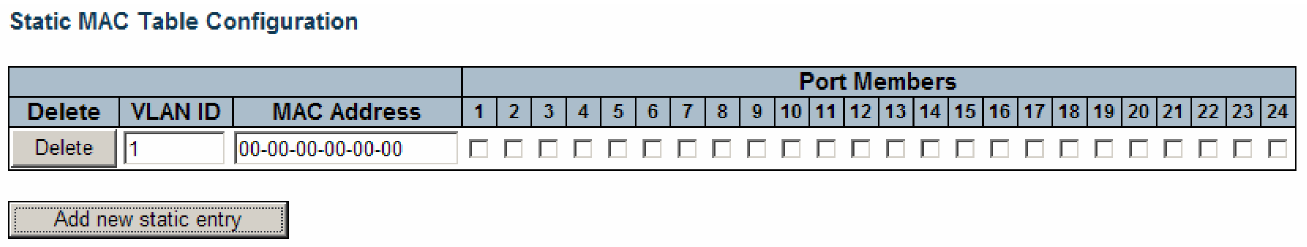
			Port Members																							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

Aging Configuration	**Description**
Disable Automatic Aging	Check to disable aging for MAC address entries.
Aging Time	Configure aging time by entering a value here in seconds Valid values: ***10 to 1000000 seconds***

Port MAC Table Learning	
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. ***Note:*** *Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.*
Add new static entry	Click to configure a new static MAC address entry in the MAC table.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.8.1 Static MAC Address Configuration



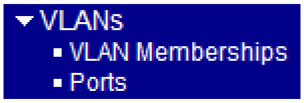
Static MAC Table Configuration

			Port Members																							
Delete	**VLAN ID**	**MAC Address**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

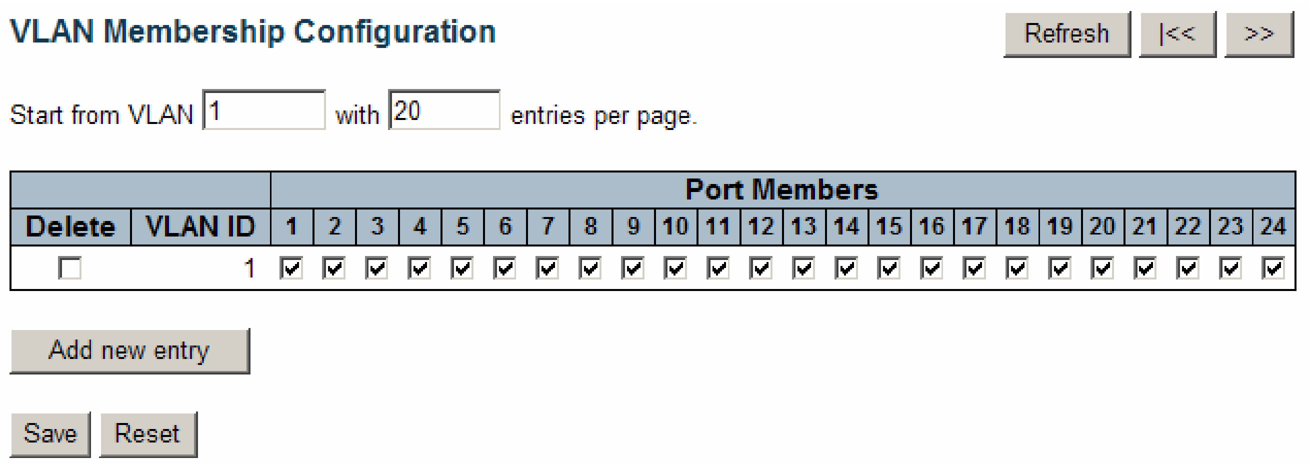
Static MAC Table Configuration	
VLAN ID	The VLAN ID for the static MAC address entry.
MAC Address	The MAC address for the entry.
Port Members	Check to indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Delete	Click to delete the entry. It will be deleted during the next save.
Add new static entry	Click to configure a new static MAC address entry in the MAC table.

2.9 VLANs

Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



2.9.1 VLAN Membership

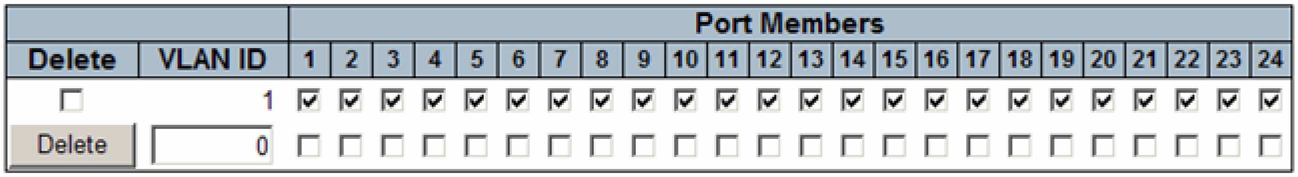

VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

		Port Members																							
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Configuration	Description
Start from VLAN …..	Select range of VLAN table entries.
Delete	Check to delete a VLAN entry. The entry will be deleted on the switch unit during the next Save.
VLAN ID	Indicates the ID of this particular VLAN.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add new entry	Click to add a new VLAN entry. An empty row is added to the table, and the VLAN can be configured as needed.
Refresh	Click to refresh the page; any changes made locally will be undone.
|<<	Click to display the first page.
>>|	Click to display the last page.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

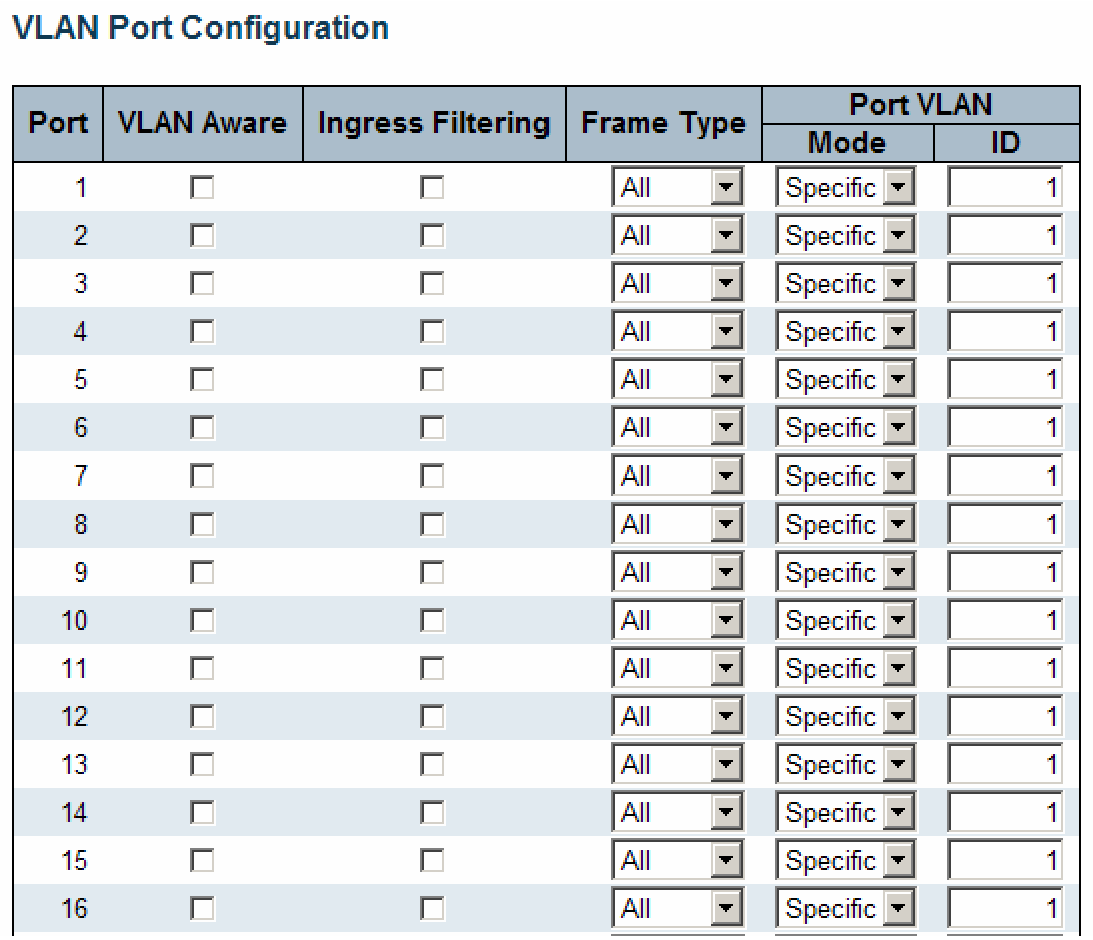
Adding a New VLAN entry



Delete	VLAN ID	Port Members																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Configuration	**Description**
VLAN ID	Enter VLAN ID for the new VLAN entry. Legal values: *1 through 4095*
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Delete	Click to delete the new VLAN row.
Add new VLAN	Click to add another new VLAN ID.
Save	Click to save the new VLAN row.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.9.2 VLAN Port Configuration



VLAN Port Configuration

Port	VLAN Aware	Ingress Filtering	Frame Type	Port VLAN	
				Mode	ID
1	☐	☐	All	Specific	1
2	☐	☐	All	Specific	1
3	☐	☐	All	Specific	1
4	☐	☐	All	Specific	1
5	☐	☐	All	Specific	1
6	☐	☐	All	Specific	1
7	☐	☐	All	Specific	1
8	☐	☐	All	Specific	1
9	☐	☐	All	Specific	1
10	☐	☐	All	Specific	1
11	☐	☐	All	Specific	1
12	☐	☐	All	Specific	1
13	☐	☐	All	Specific	1
14	☐	☐	All	Specific	1
15	☐	☐	All	Specific	1
16	☐	☐	All	Specific	1

Configuration	Description
Port	This is the logical port number for this row.
VLAN Aware	Enable VLAN awareness for a port by checking the box. This parameter affects VLAN ingress processing. If VLAN awareness is enabled: the tag is removed from tagged frames received on the port. Furthermore, VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed. By default, VLAN awareness is disabled (no checkmark).
Ingress Filtering	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
Frame Type	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. ***All:*** all frames are accepted. (Default)

Tagged: Only tagged frames are accepted. Untagged frames received on the port are discarded.

Port VLAN Mode

Configures the Port VLAN Mode. This parameter affects VLAN ingress and egress processing.

None: a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches.

Specific: (the default value) a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID

Configures the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1.

Note: *The port must be a member of the same VLAN as the Port VLAN ID.*

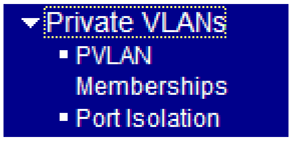
Save

Click to save the changes.

Reset

Click to undo any changes made locally and revert to previously saved values.

2.10 Private VLANs



A **Private VLAN** is a VLAN which contains switched ports that are restricted, such that they can only communicate with a given "uplink", or called “Promiscuous port”. The restricted ports are called "Isolated ports". Each private VLAN typically contains many isolated ports, and a single uplink. The uplink will typically be a switched port (or link aggregation group) connected to a router, firewall, server, provider network, or similar central resource.

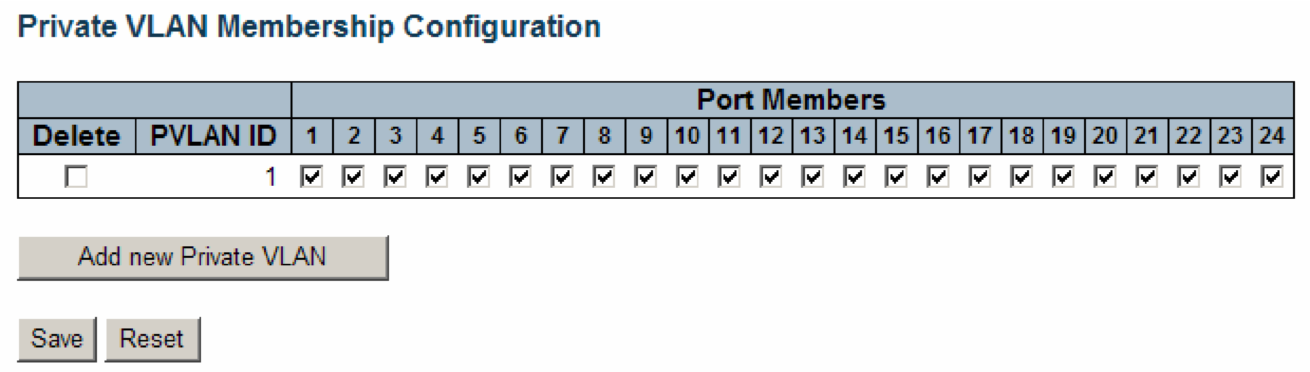
Types of Ports in a private VLAN

Promiscuous: Usually connects to a router – a type of a port which is allowed to send and receive frames from any other port on the VLAN.

Isolated: This type of port is only allowed to communicate with Promiscuous ports. Isolated ports are not allowed to communicate to each other. This type of ports usually connects to hosts.

By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

2.10.1 PVLAN Memberships

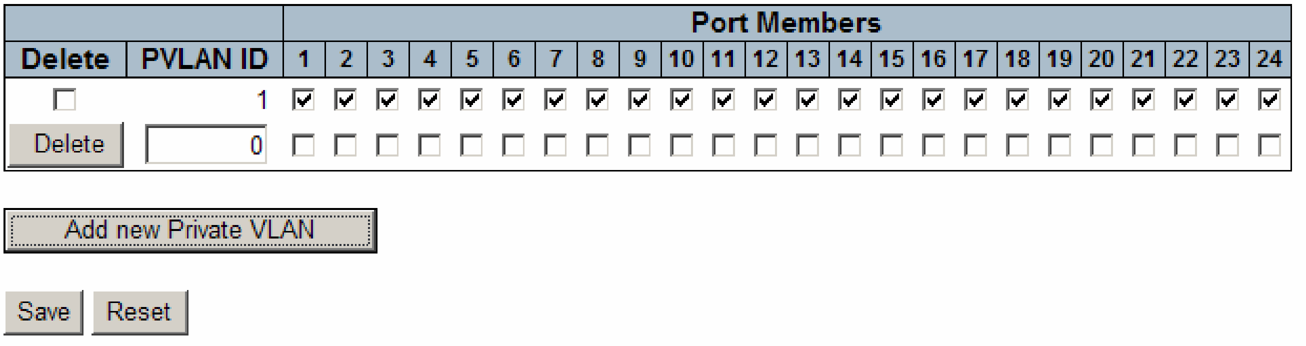


Private VLAN Membership Configuration

		Port Members																							
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Configuration	Description
Delete	Check to delete a VLAN entry. The entry will be deleted on the switch unit during
Private VLAN ID	Indicates the ID of this particular private VLAN. *Note: The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears.*
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add new Private VLAN	Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

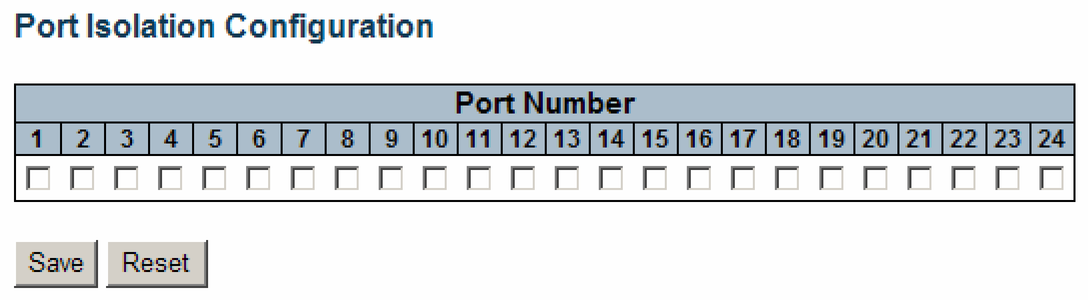
Adding new Private VLAN



		Port Members																							
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Configuration	**Description**
Private VLAN ID	See above.
Port Members	See above.
Delete	Click to delete the new private VLAN row.

2.10.2 Port Isolation



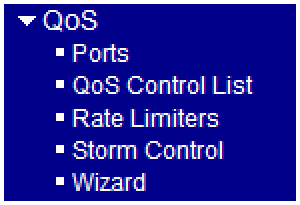
Port Isolation Configuration

Port Number																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

A port member of a VLAN can be isolated to other isolated ports on Private VLAN.

Configuration	Description
Port Numbers	A check box is provided for each port of a private VLAN. When checked, set the port to be isolation port in a private VLAN. When unchecked, set the port to be promiscuous port in a private VLAN. By default, port isolation is disabled for all ports.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

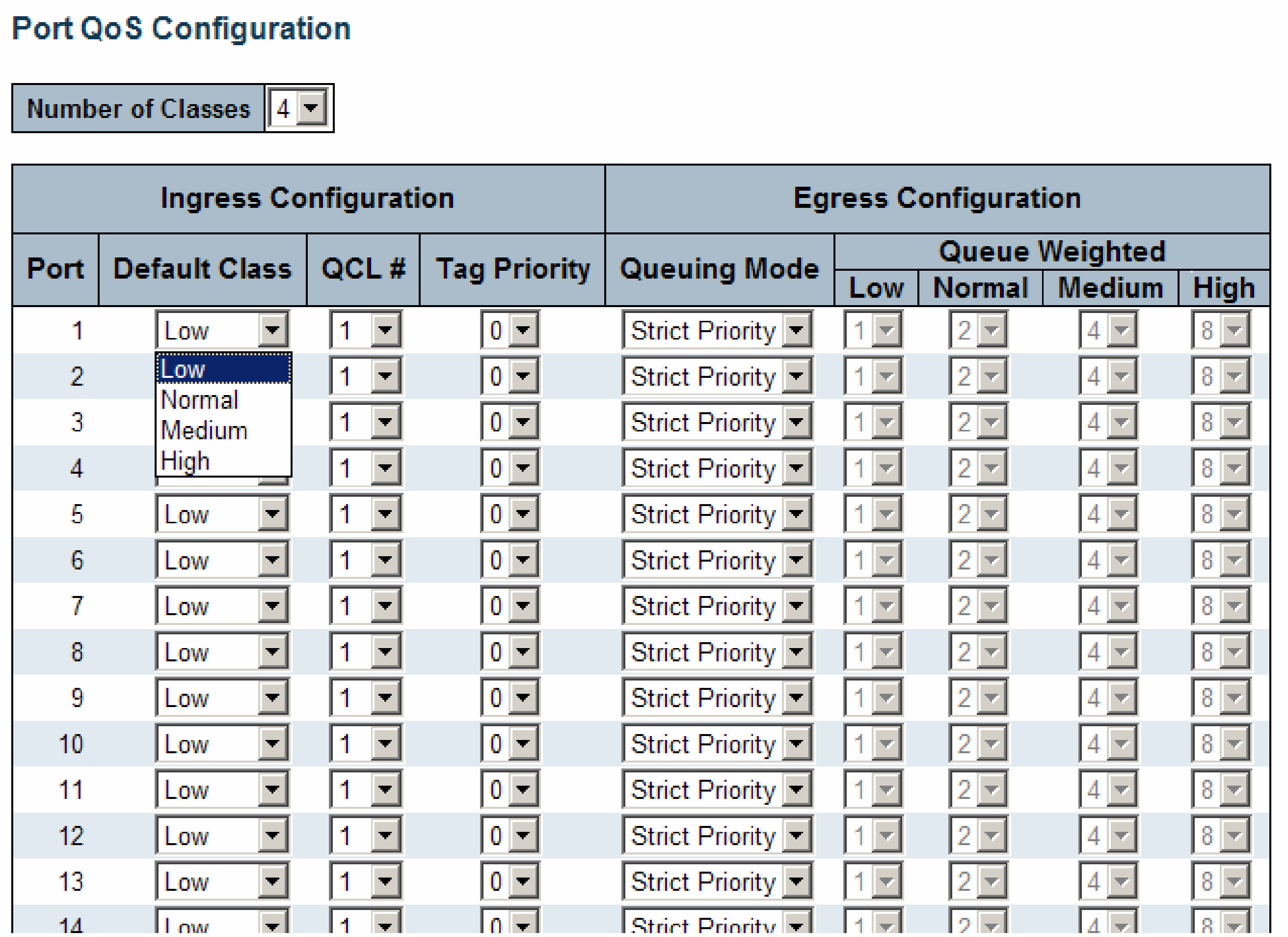
2.11 QoS



Frames can be classified by 4 different QoS classes: ***Low***, ***Normal***, ***Medium***, and ***High***.
The classification is controlled by a QCL that is assigned to each port. A QCL consists of an ordered list of up to 12 QCEs. Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS class for the port.

2.11.1 Ports



Port QoS Configuration

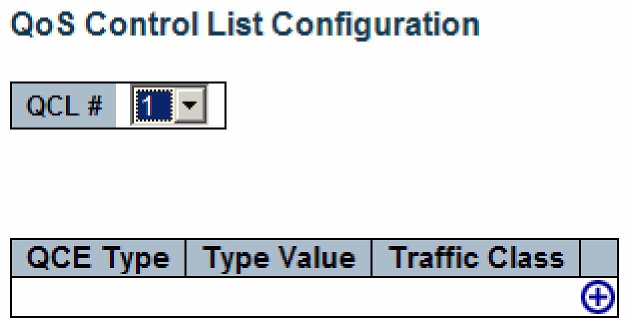
Number of Classes: 4

Ingress Configuration				Egress Configuration				
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2		1	0	Strict Priority	1	2	4	8
3		1	0	Strict Priority	1	2	4	8
4		1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8

Configuration	Description
Number of Classes	Configure the number of traffic classes as "1", "2", or "4". The default value is "4".
Ingress Configuration	
Port	The logical port for the settings contained in the same row.
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL #	Select which QCL to use for the port.
Tag Priority	Select the default tag priority for this port when adding a Tag to the untagged frames.
Egress Configuration	
Queuing Mode	Select which Queuing mode for this port. ***Strict Priority:*** High class queue is served first always till it is empty ***Weighted:*** The queues are served based on the weight ratios set below.
Queue Weighted	Setting Queue weighted (Low:Normal:Medium:High) if the "Queuing Mode" is "Weighted".

- Low	Weight of ***Low*** Class
- Normal	Weight of ***Normal*** Class
- Medium	Weight of ***Medium*** Class
- High	Weight of ***High*** Class
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.11.2 QoS Control List

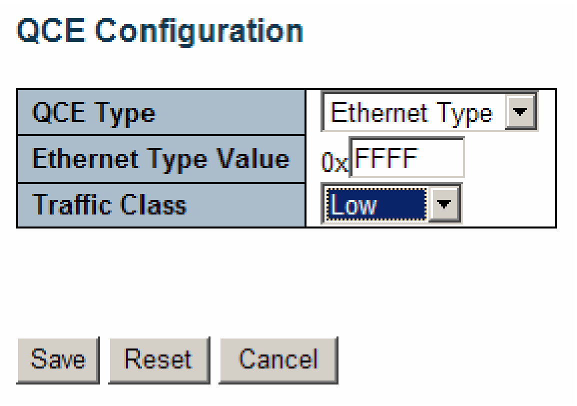


QoS Control List Configuration

QCL # 1

QCE Type	Type Value	Traffic Class	
			⊕

Configuration	Description
QCL #	Select a QCL to display a table that lists all the QCEs for that particular QCL.
	You can modify each QCE in the table using the following buttons:
(+)	Inserts a new QCE before the current row.
(e)	Edits the QCE.
(↑)	Moves the QCE up the list.
(↓)	Moves the QCE down the list.
(X)	Deletes the QCE.
(+)	The lowest plus sign adds a new entry at the bottom of the list of QCL.

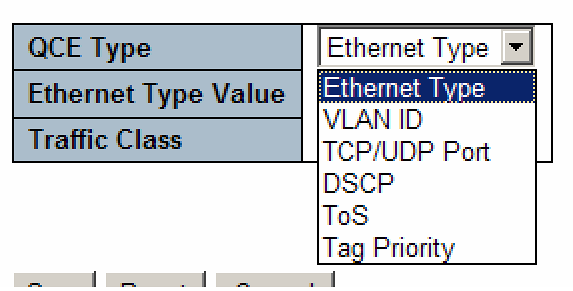


QCE Configuration

QCE Type	Ethernet Type
Ethernet Type Value	0xFFFF
Traffic Class	Low

QCE Type	Specifies which frame field the QCE processes to determine the QoS class of the

frame. The following QCE types are supported:



QCE Type	Ethernet Type
Ethernet Type Value	
Traffic Class	

***Ethernet Type*:** The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header.

VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged.

TCP/UDP Port: IPv4 TCP/UDP source/destination port.

DSCP: IPv4 and IPv6 DSCP.

***ToS*:** The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field).

Tag Priority: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.

Type Value

Indicates the value according to its QCE type.

Traffic Class

The QoS class associated with the QCE.

Save

Click to save the changes.

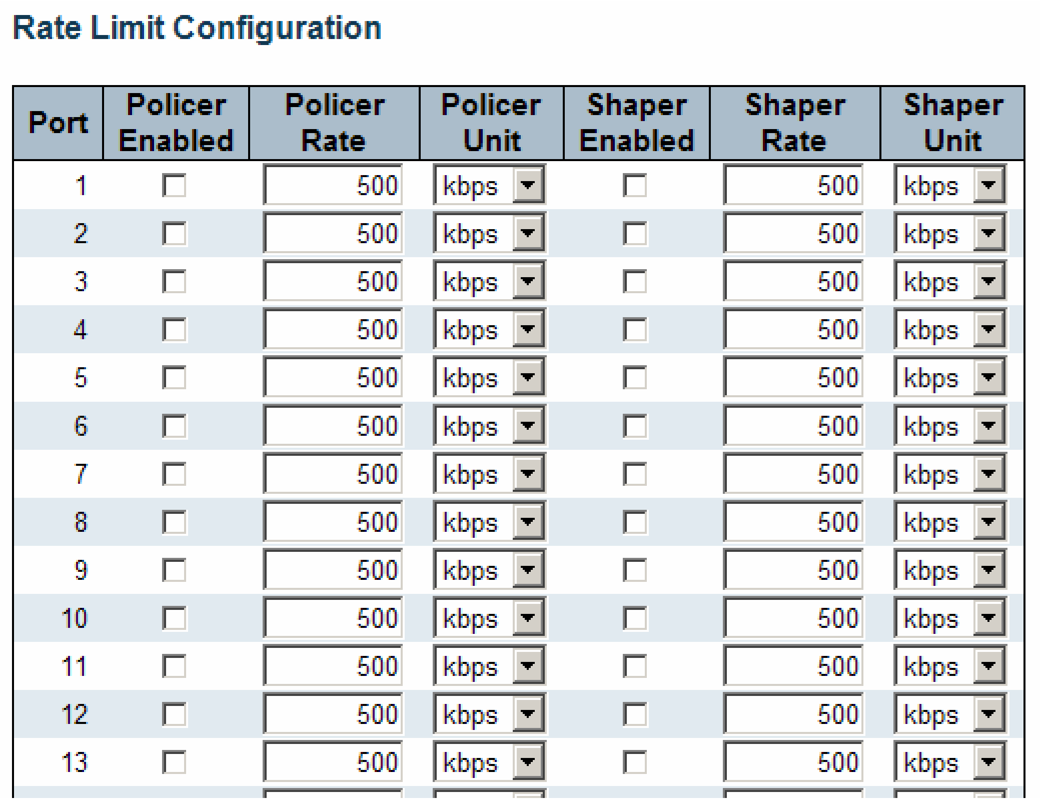
Reset

Click to undo any changes made locally and revert to previously saved values.

Cancel

Click to return to previous page.

2.11.3 Rate Limiters



Rate Limit Configuration

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	□	500	kbps	□	500	kbps
2	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps
9	□	500	kbps	□	500	kbps
10	□	500	kbps	□	500	kbps
11	□	500	kbps	□	500	kbps
12	□	500	kbps	□	500	kbps
13	□	500	kbps	□	500	kbps

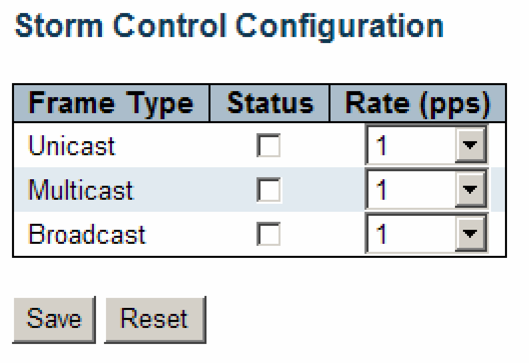
Configuration	**Description**
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to ***500-1000000*** when the "Policer Unit" is "kbps", and it is restricted to ***1-1000*** when the "Policer Unit" is "Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to ***500-1000000*** when the "Policer Unit" is "kbps", and it is restricted to ***1-1000*** when the "Policer Unit" is "Mbps".
Shaper Unit	Configure the unit of measure for the port shaper rate as ***kbps*** or ***Mbps***. The default value is "kbps".
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.11.4 Storm Control

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilo-packets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.

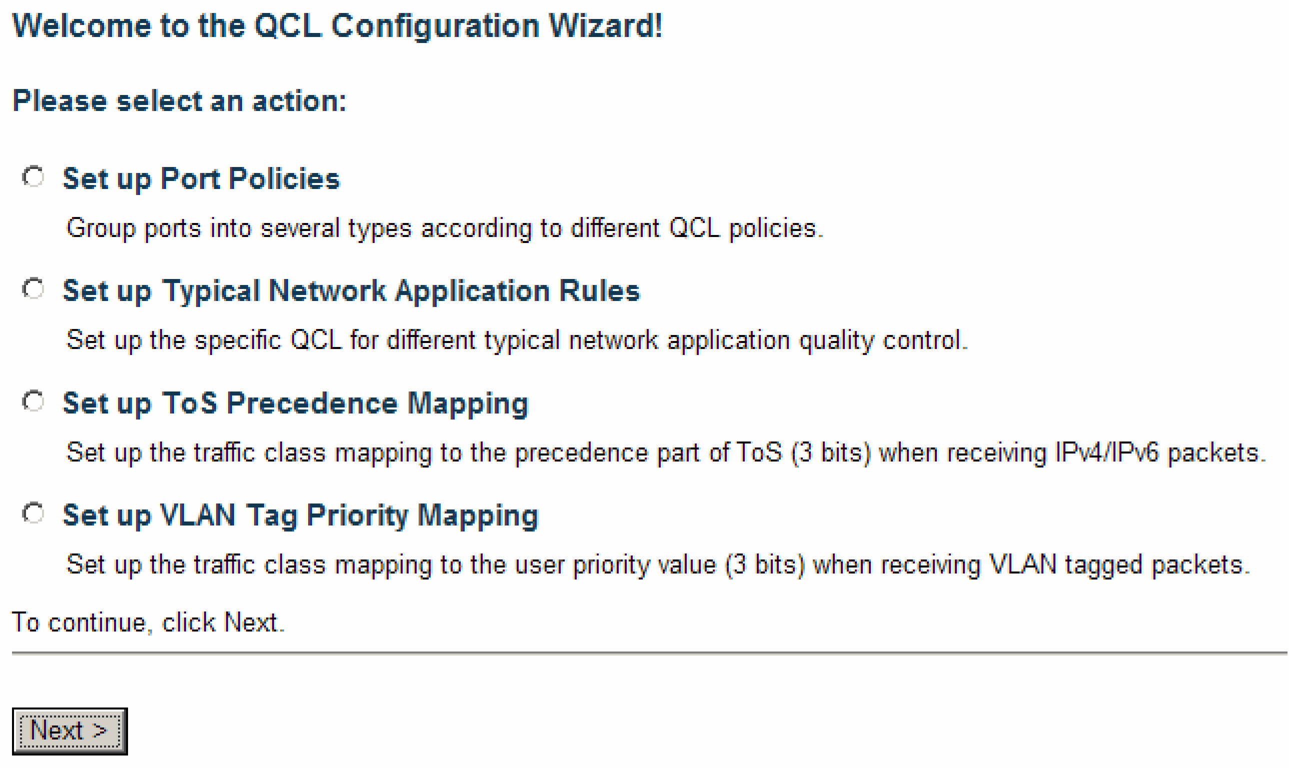


Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

Configuration	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as ***1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K,*** or ***1024K***. The 1 kpps is actually 1002.1 pps.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.11.5 Wizard



Welcome to the QCL Configuration Wizard!

Please select an action:

○ Set up Port Policies

Group ports into several types according to different QCL policies.

○ Set up Typical Network Application Rules

Set up the specific QCL for different typical network application quality control.

○ Set up ToS Precedence Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.

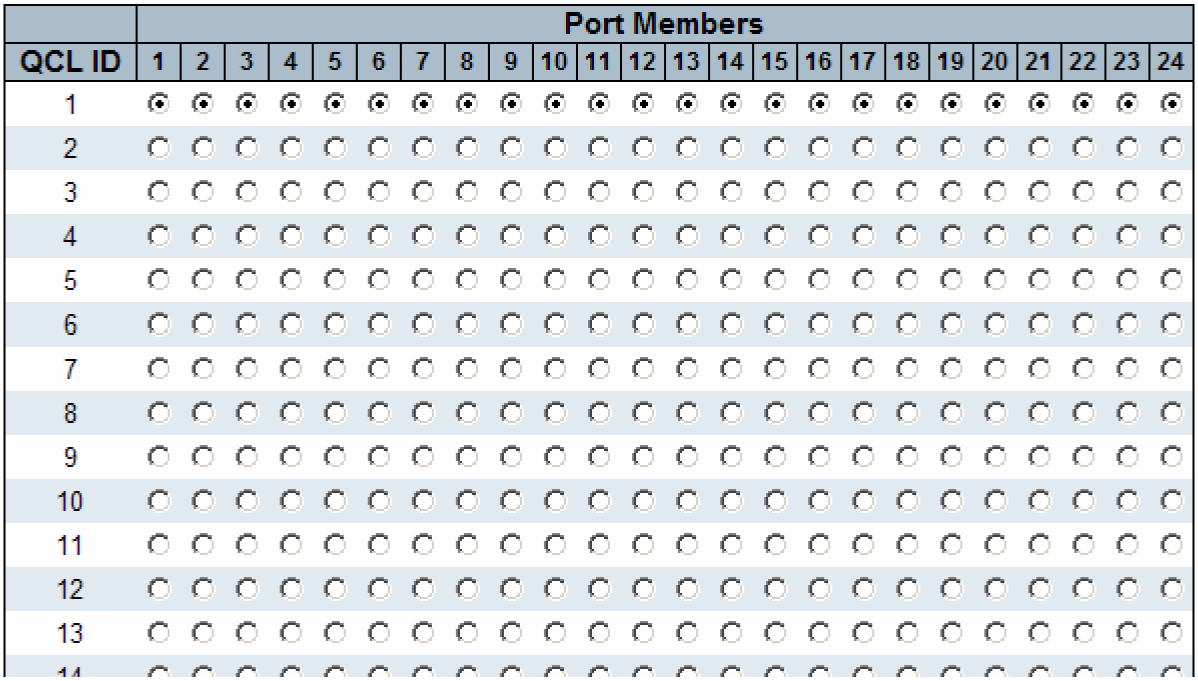
○ Set up VLAN Tag Priority Mapping

Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

To continue, click Next.

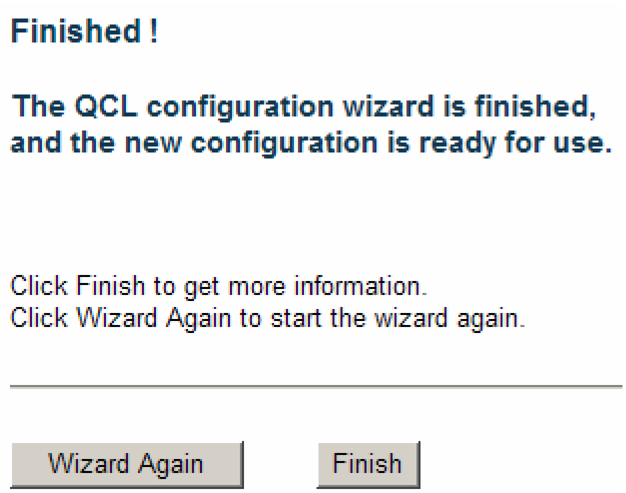
This handy wizard helps you set up a QCL quickly.

2.11.6 Wizard – Port Policies



	Port Members																						
QCL ID	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
13	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
14	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Configuration	**Description**
QCL ID	Frames that hit this QCE are set to match this specific QCL.
Port Members	A row of radio buttons for each port is displayed for each QCL ID. To include a port in a QCL member, click the radio button.
Cancel Wizard	Click to cancel the wizard.
< Back	Click to go back to the previous wizard step.
Next >	Click to continue the wizard.

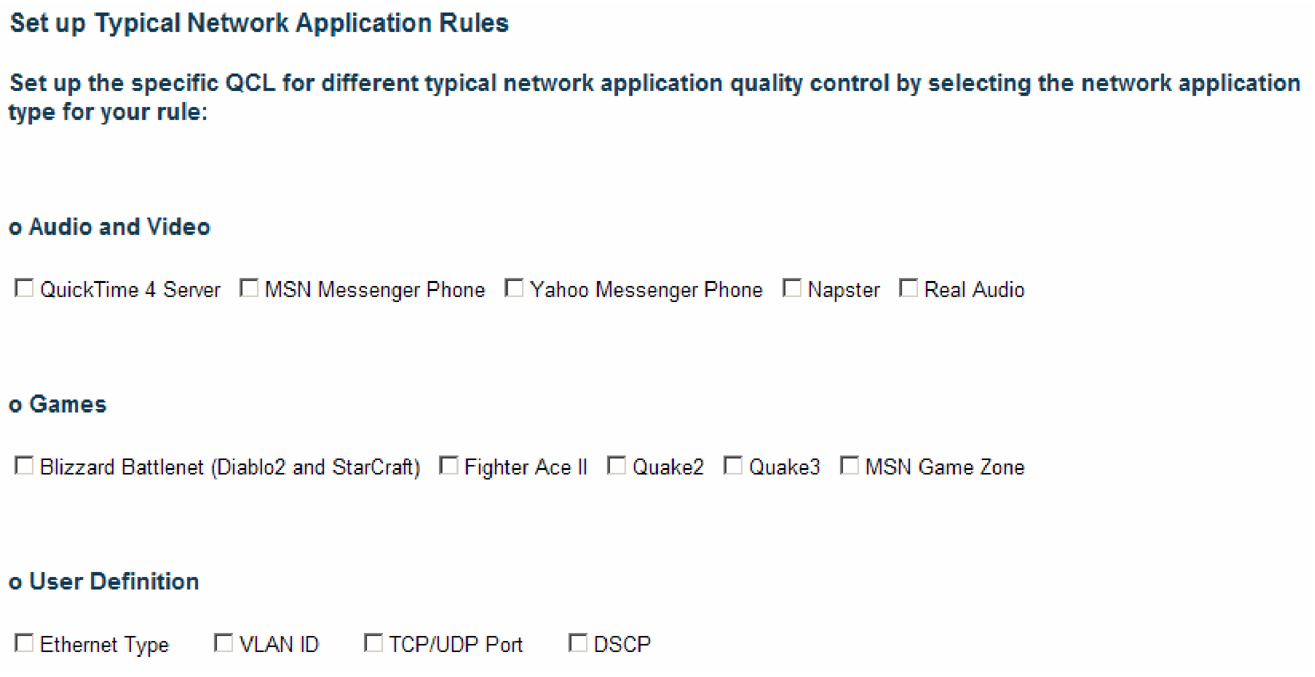


Finished !

The QCL configuration wizard is finished, and the new configuration is ready for use.

Click Finish to get more information.
Click Wizard Again to start the wizard again.

2.11.7 Wizard – Typical Network Application Rules



Set up Typical Network Application Rules

Set up the specific QCL for different typical network application quality control by selecting the network application type for your rule:

o Audio and Video

□ QuickTime 4 Server □ MSN Messenger Phone □ Yahoo Messenger Phone □ Napster □ Real Audio

o Games

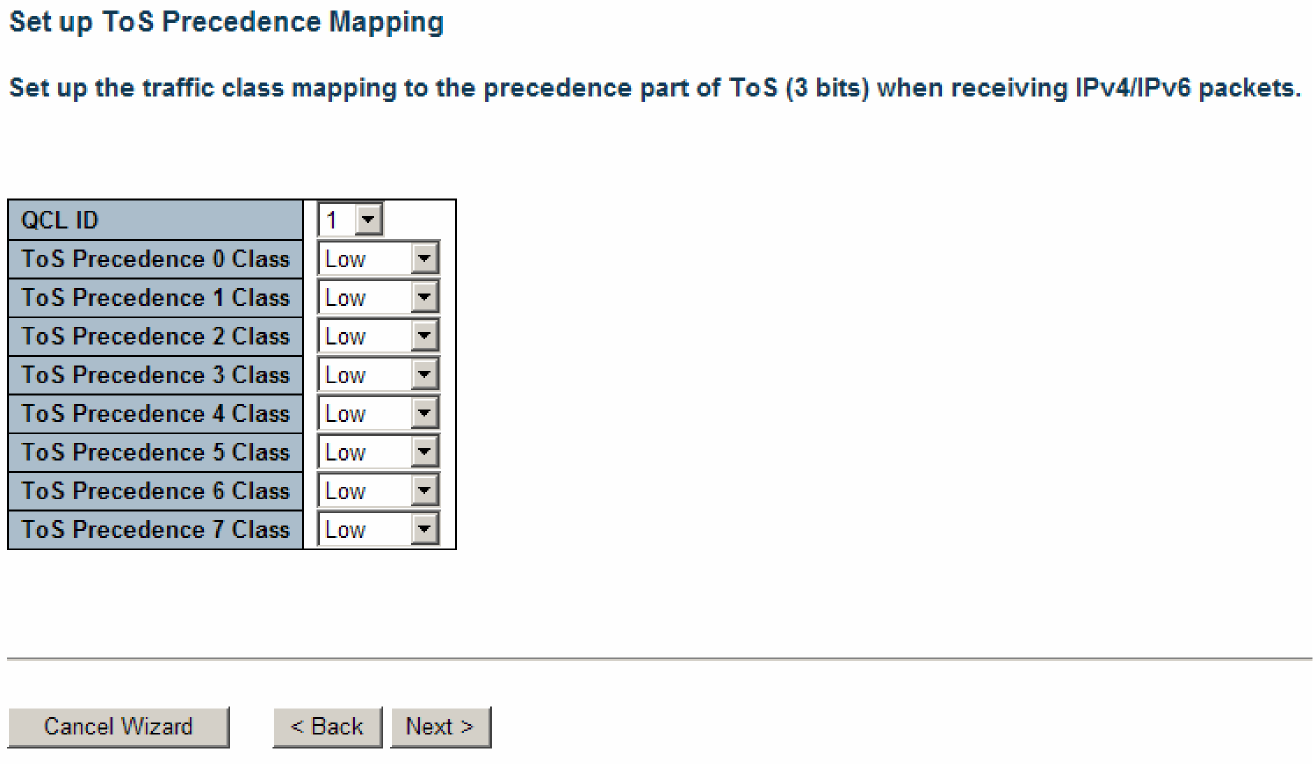
□ Blizzard Battlenet (Diablo2 and StarCraft) □ Fighter Ace II □ Quake2 □ Quake3 □ MSN Game Zone

o User Definition

□ Ethernet Type □ VLAN ID □ TCP/UDP Port □ DSCP

Configuration	Description
Audio and Video	Indicates the common servers that apply to the specific QCE . The common servers are: *QuickTime 4 Server, MSN Messenger Phone, Yahoo Messenger Phone, Napster, Real Audio*.
Games	Indicates the common games that apply to the specific QCE.
User Definition	Indicates the user definition that applies to the specific QCE. The user definitions are: ***Ethernet Type:*** Specify the Ethernet Type filter for this QCE. The allowed range is *0x600* to *0xFFFF*. ***VLAN ID:*** VLAN ID filter for this QCE. The allowed range is *1* to *4095*. ***UDP/TCP Port:*** Specify the TCP/UDP port filter for this QCE. The allowed range is *0* to *65535*. ***DSCP:*** Specify the DSCP filter for this QCE. The allowed range is *0* to *63*.
Cancel Wizard	Click to cancel the wizard.
< Back	Click to go back to the previous wizard step.
Next >	Click to continue the wizard.

2.11.8 Wizard – ToS Precedence Mapping



Set up ToS Precedence Mapping

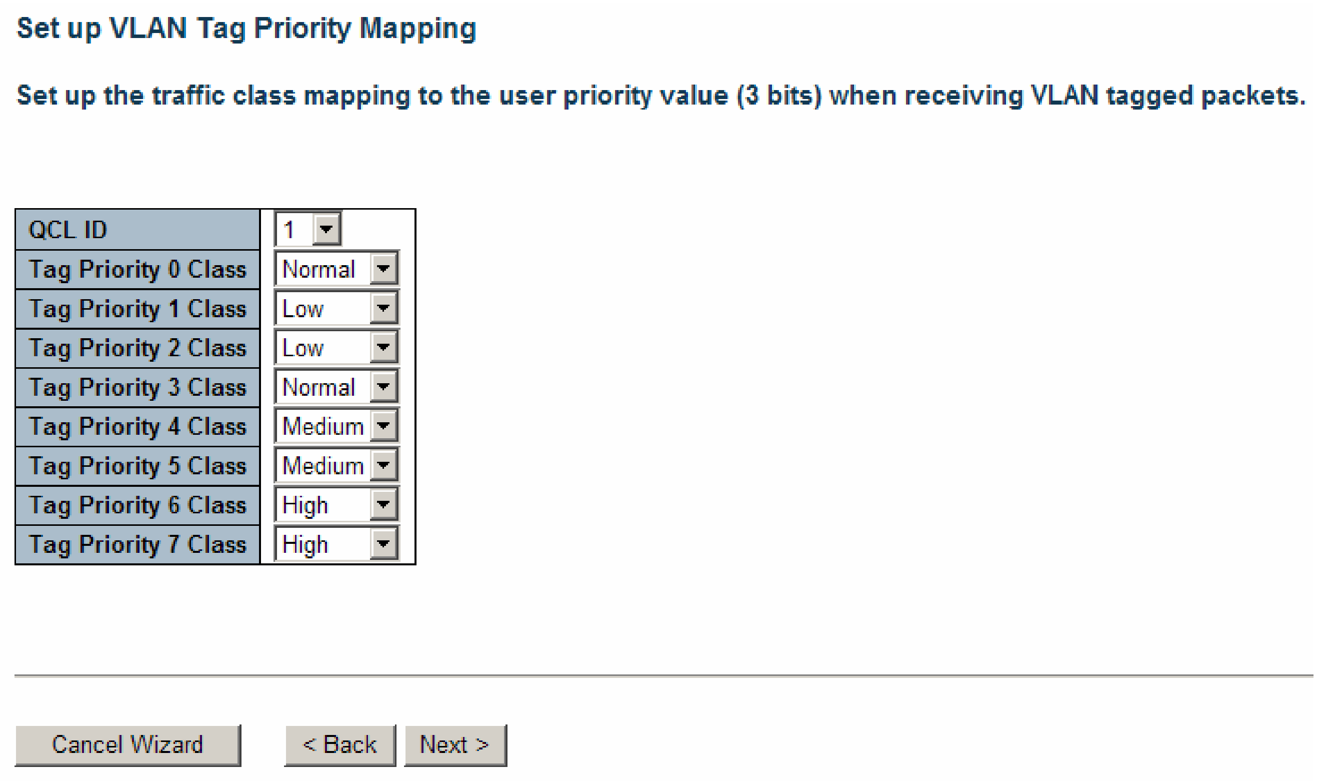
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.

QCL ID	1
ToS Precedence 0 Class	Low
ToS Precedence 1 Class	Low
ToS Precedence 2 Class	Low
ToS Precedence 3 Class	Low
ToS Precedence 4 Class	Low
ToS Precedence 5 Class	Low
ToS Precedence 6 Class	Low
ToS Precedence 7 Class	Low

This wizard is used to set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.

Configuration	Description
QCL ID	Select the QCL ID to which this QCE applies.
ToS Precedence Class	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.
Cancel Wizard	Click to cancel the wizard.
< Back	Click to go back to the previous wizard step.
Next >	Click to continue the wizard.

2.11.9 Wizard – VLAN Tag Priority Mapping



Set up VLAN Tag Priority Mapping

Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

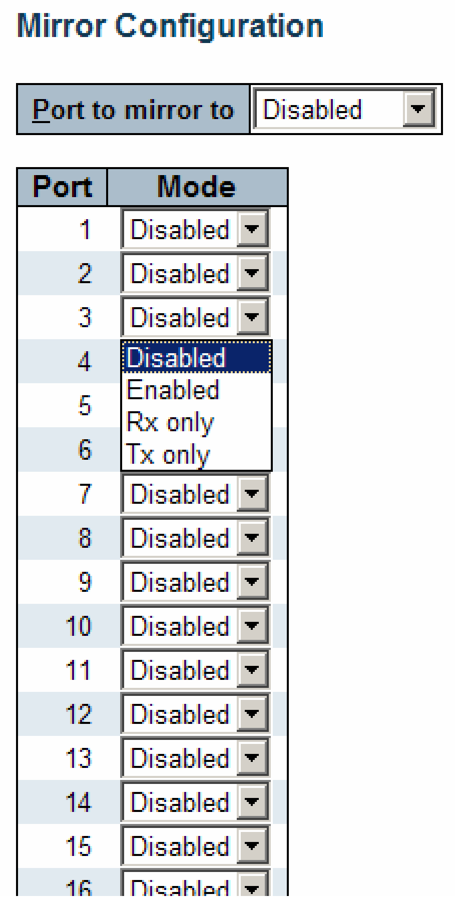
QCL ID	1
Tag Priority 0 Class	Normal
Tag Priority 1 Class	Low
Tag Priority 2 Class	Low
Tag Priority 3 Class	Normal
Tag Priority 4 Class	Medium
Tag Priority 5 Class	Medium
Tag Priority 6 Class	High
Tag Priority 7 Class	High

Configuration	Description
QCL ID	Select the QCL ID to which this QCE applies.
VLAN Priority Class	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.
Cancel Wizard	Click to cancel the wizard.
< Back	Click to go back to the previous wizard step.
Next >	Click to continue the wizard.

2.12 Mirroring

To debug network problems, selected traffic can be copied, or mirrored, to a **mirror port** where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied to the **mirror port** is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).



Mirror Configuration

Port to mirror to	Disabled

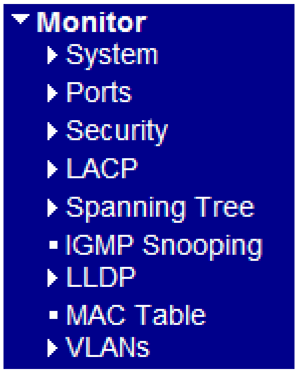
Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	
6	
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled

Configuration	Description
Port to mirror to	**Port to mirror** is also known as the **mirror port**. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.
Port	The logical port for the settings contained in the same row.
Mode	Select one of the following mirror modes. ***Rx only:*** Frames received at this port are mirrored to the **mirror port**. Frames transmitted are not mirrored. ***Tx only:*** Frames transmitted from this port are mirrored to the **mirror port**. Frames received are not mirrored.

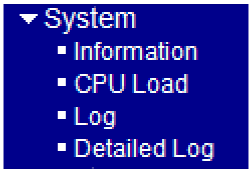
	Disabled: Neither frames transmitted nor frames received are mirrored. ***Enabled:*** Frames received and frames transmitted are mirrored to the **mirror port**.
Save	Click to save the changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the ***mirror port****. Because of this,* ***mode*** *for the selected* ***mirror port*** *is limited to Disabled or Rx only.*

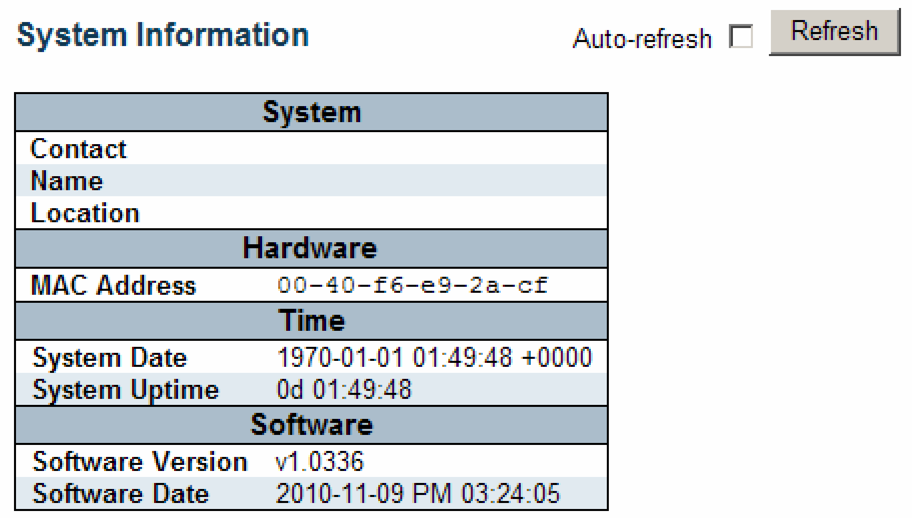
3. Monitor



3.1 System



3.1.1 Information



System Information

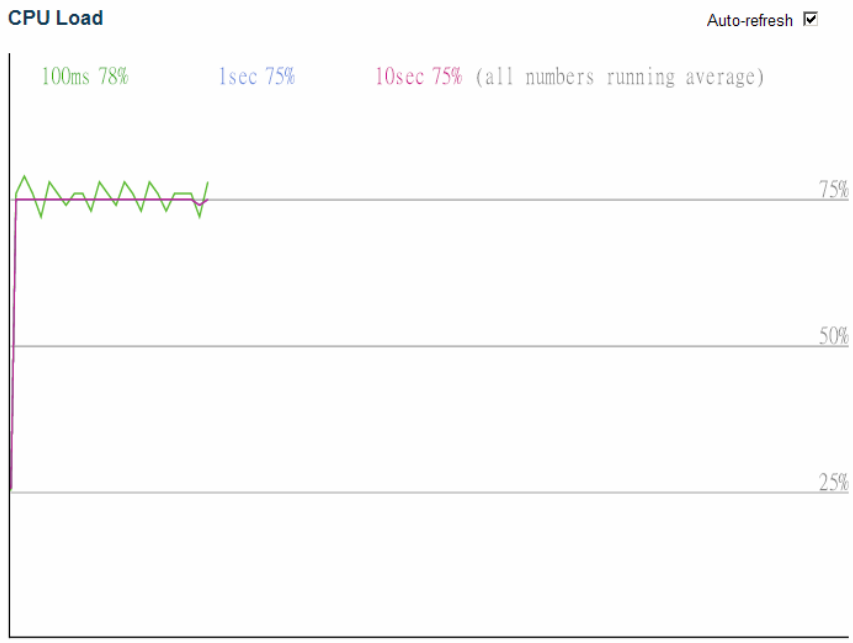
System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-40-f6-e9-2a-cf
Time	
System Date	1970-01-01 01:49:48 +0000
System Uptime	0d 01:49:48
Software	
Software Version	v1.0336
Software Date	2010-11-09 PM 03:24:05

Status Information	Description
Contact	The system contact configured in Configuration | System | Information | System Contact.
Name	The system name configured in Configuration | System | Information | System Name.
Location	The system location configured in Configuration | System | Information | System Location.
MAC Address	The MAC Address of this switch.

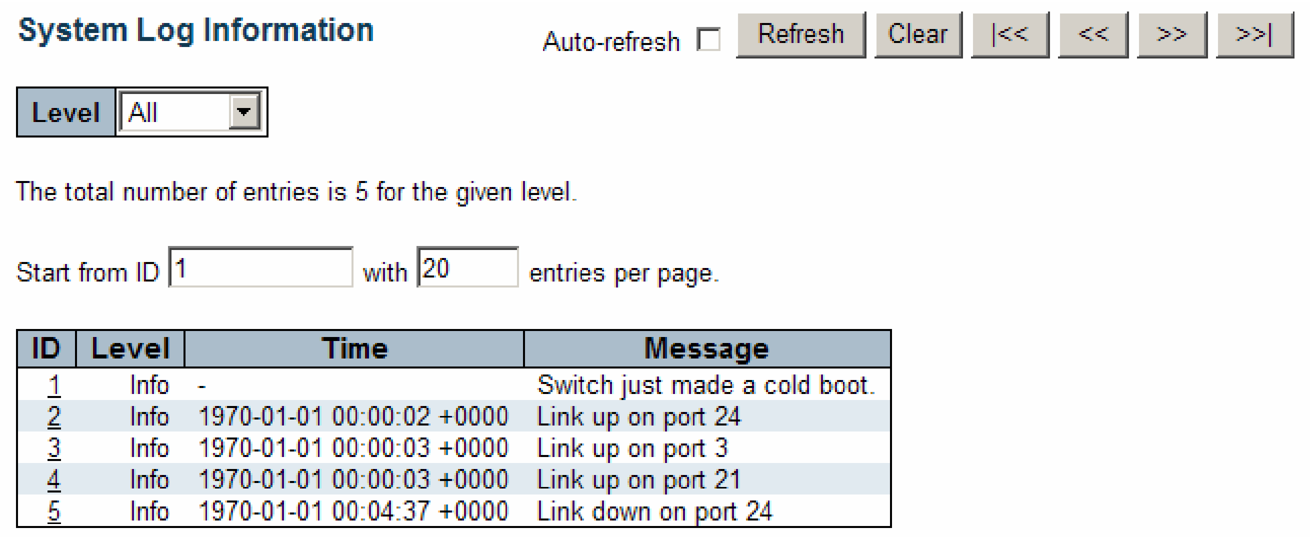
System Date	The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.
System Uptime	The period of time the device has been operational.
Switch ID	The switch ID.
Software Version	The software version of the switch
Software Date	The date when the switch software was produced.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.1.2 CPU Load

This page displays the CPU load, using a SVG graph. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plug-in installed to support SVG.



3.1.3 Log



System Log Information

Level: All

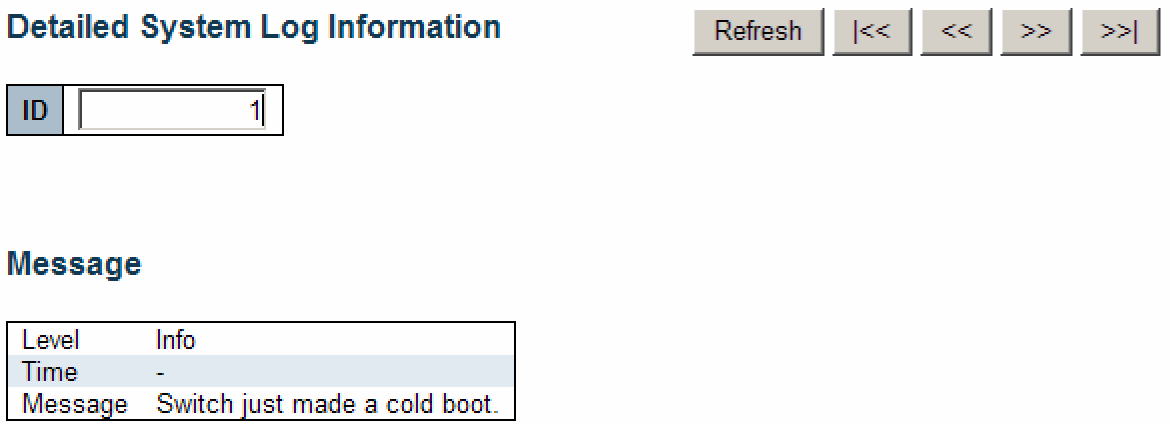
The total number of entries is 5 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Info	-	Switch just made a cold boot.
2	Info	1970-01-01 00:00:02 +0000	Link up on port 24
3	Info	1970-01-01 00:00:03 +0000	Link up on port 3
4	Info	1970-01-01 00:00:03 +0000	Link up on port 21
5	Info	1970-01-01 00:04:37 +0000	Link down on port 24

Configuration	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: ***Info:*** Information level of the system log. ***Warning:*** Warning level of the system log. ***Error:*** Error level of the system log. ***All:*** All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
I<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending from the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>> I	Updates the system log entries, ending at the last entry currently displayed.

3.1.4 Detailed Log



Detailed System Log Information

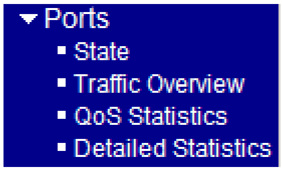
ID: 1

Message

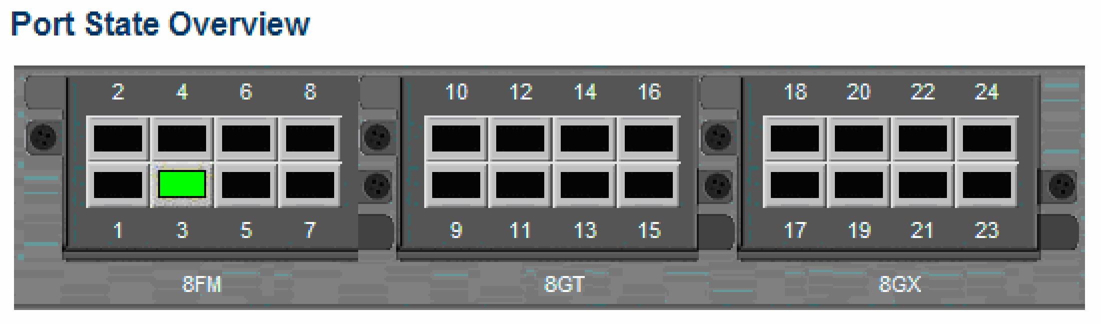
Level	Info
Time	-
Message	Switch just made a cold boot.

Configuration	Description
ID	The ID (>= 1) of the system log entry.
Message	The message of the system log entry.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
I<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending from the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>> I	Updates the system log entries, ending at the last entry currently displayed.

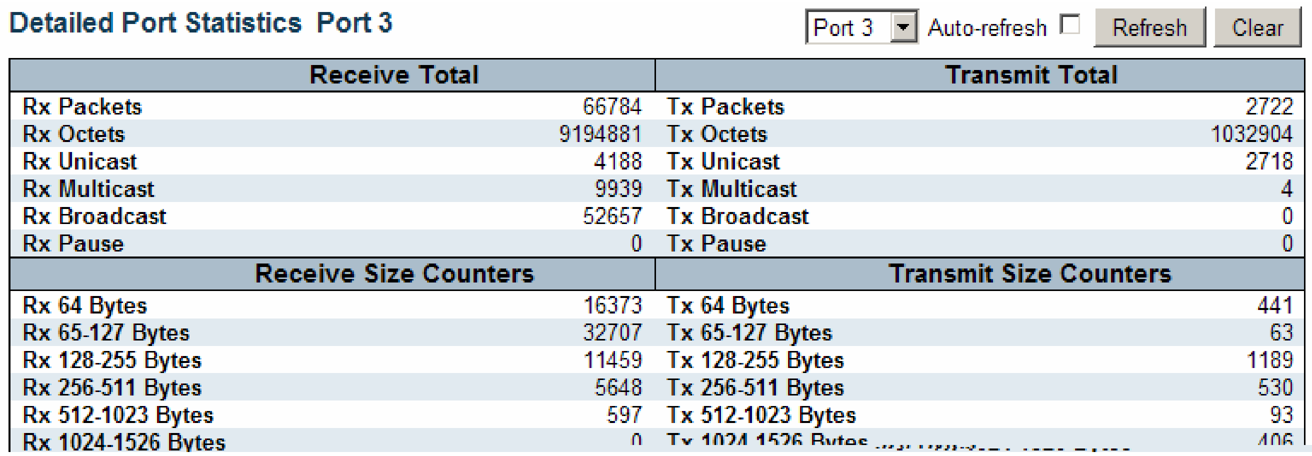
3.2 Ports



3.2.1 State



Configuration	Description
Port Icon	Click the port icon to display its detailed statistics. Port 3 example:

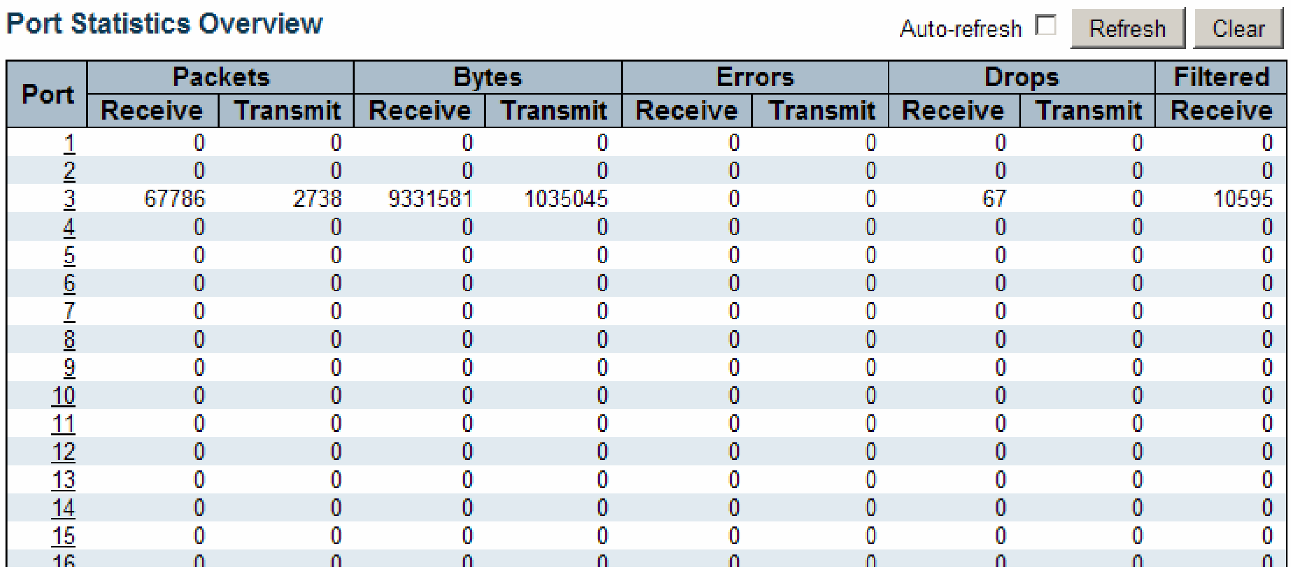


Detailed Port Statistics Port 3

Receive Total		Transmit Total	
Rx Packets	66784	Tx Packets	2722
Rx Octets	9194881	Tx Octets	1032904
Rx Unicast	4188	Tx Unicast	2718
Rx Multicast	9939	Tx Multicast	4
Rx Broadcast	52657	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	16373	Tx 64 Bytes	441
Rx 65-127 Bytes	32707	Tx 65-127 Bytes	63
Rx 128-255 Bytes	11459	Tx 128-255 Bytes	1189
Rx 256-511 Bytes	5648	Tx 256-511 Bytes	530
Rx 512-1023 Bytes	597	Tx 512-1023 Bytes	93
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	406

Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.2.2 Traffic Overview

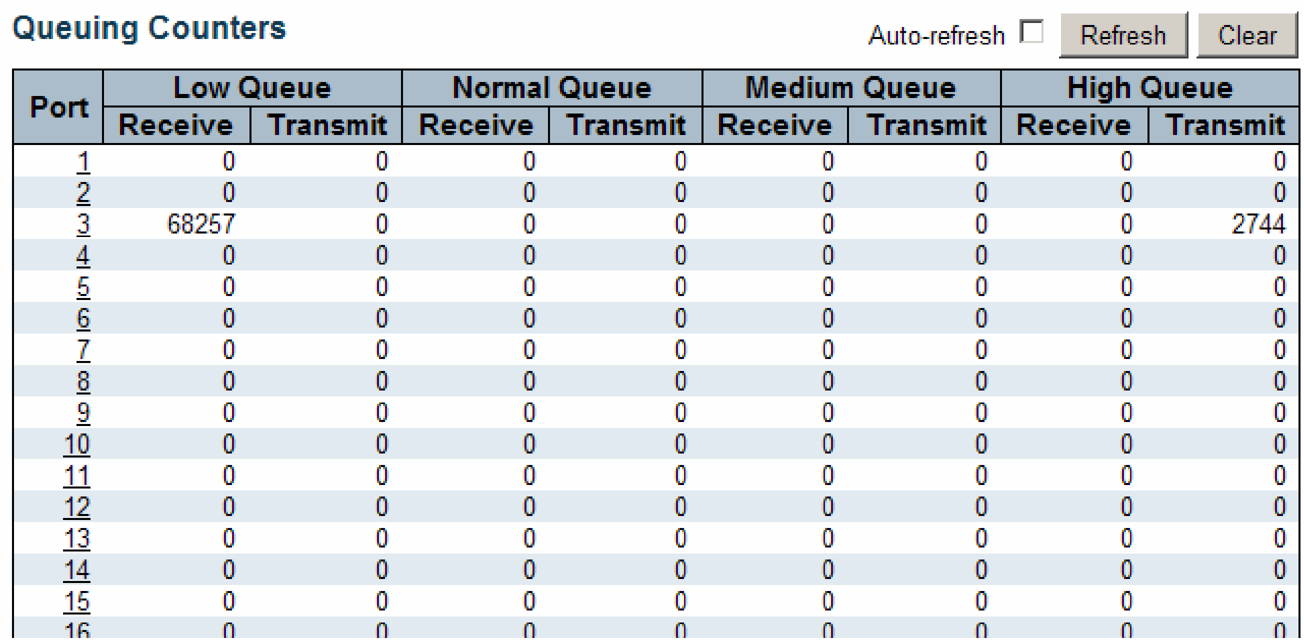


Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	67786	2738	9331581	1035045	0	0	67	0	10595
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0

Configuration	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.\
Bytes	The number of received and transmitted bytes per port
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process
Receive/Transmit	The number of received and transmitted packets per port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to flush all counters.

3.2.3 QoS Statistics

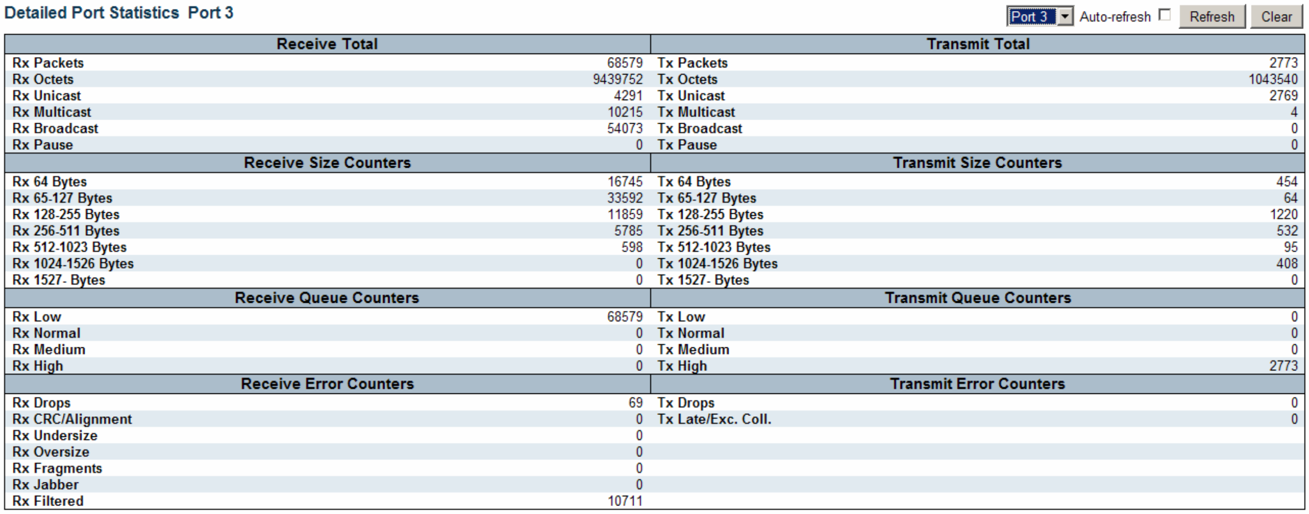


Queuing Counters

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	68257	0	0	0	0	0	0	2744
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0

Configuration	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
Medium Queue	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
High Queue	This is the highest priority queue of the 4 QoS queues.
Receive/Transmit	The number of received and transmitted packets per port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to flush all counters.

3.2.4 Detailed Statistics



Detailed Port Statistics Port 3

Receive Total		Transmit Total	
Rx Packets	68579	Tx Packets	2773
Rx Octets	9439752	Tx Octets	1043540
Rx Unicast	4291	Tx Unicast	2769
Rx Multicast	10215	Tx Multicast	4
Rx Broadcast	54073	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	16745	Tx 64 Bytes	454
Rx 65-127 Bytes	33592	Tx 65-127 Bytes	64
Rx 128-255 Bytes	11859	Tx 128-255 Bytes	1220
Rx 256-511 Bytes	5785	Tx 256-511 Bytes	532
Rx 512-1023 Bytes	598	Tx 512-1023 Bytes	95
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	408
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Low	68579	Tx Low	0
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	2773
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	69	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	10711		

Configuration	Description
Receive Total and Transmit Total	
Rx and Tx Packets	Number of received and transmitted (good and bad) packets.
Rx and Tx Octets	Number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	Number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	Number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	Number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	Counter of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	
	Number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.
Receive and Transmit Queue Counters	
	Number of packets received and transmitted by the input and output queues.
Receive Error Counters	
Rx Drops	Number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	Number of frames received with CRC or alignment errors.
Rx Undersize	Number of short [1] frames received with valid CRC.
Rx Oversize	Number of long [2] frames received with valid CRC.
Rx Fragments	Number of short [1] frames received with invalid CRC.
Rx Jabber	Number of long [2] frames received with invalid CRC.

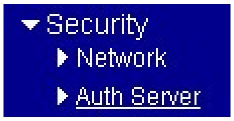
Rx Filtered	Number of received frames filtered by the forwarding process.
Transmit Error Counters	
Tx Drops	Number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	Number of frames dropped due to excessive or late collisions.
Port #	Select the logical port for the displayed statistics
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to flush all counters.

Note:

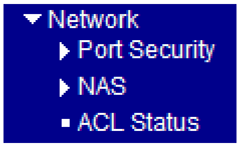
[1] *Short frames are frames that are smaller than 64 bytes.*

[2] *Long frames are frames that are longer than the configured maximum frame length for this port.*

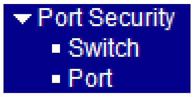
3.3 Security



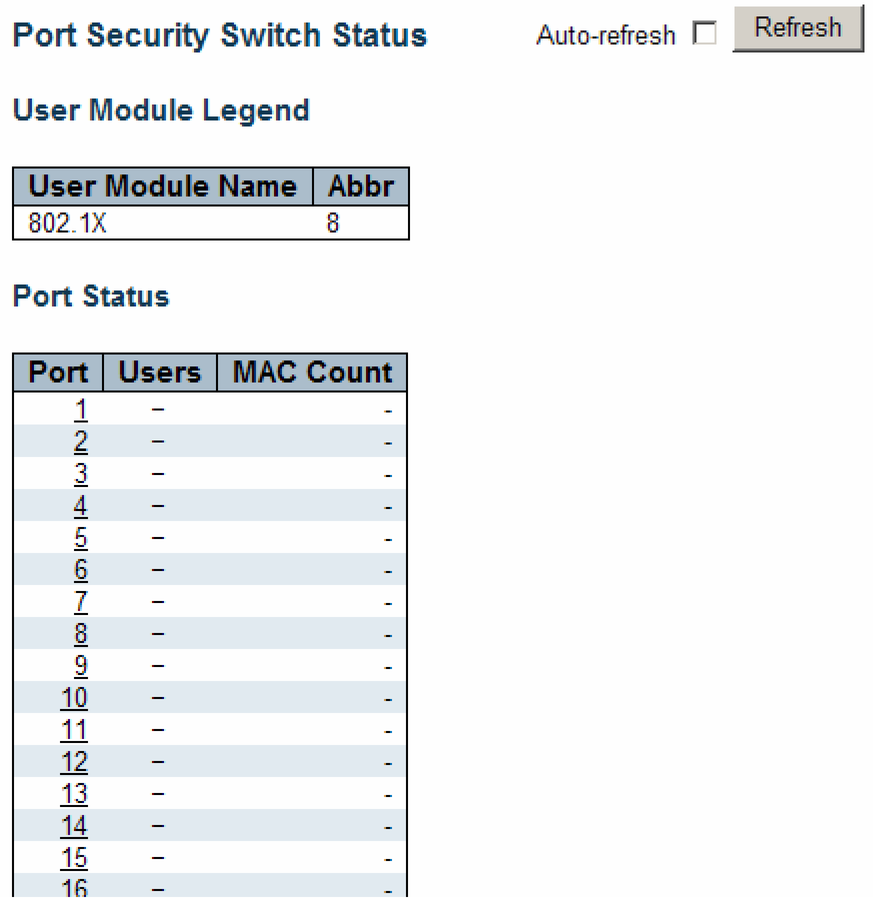
3.3.1 Network



3.3.1.1 Port Security



3.3.1.1.1 Switch



Port Security Switch Status

User Module Legend

User Module Name	Abbr
802.1X	8

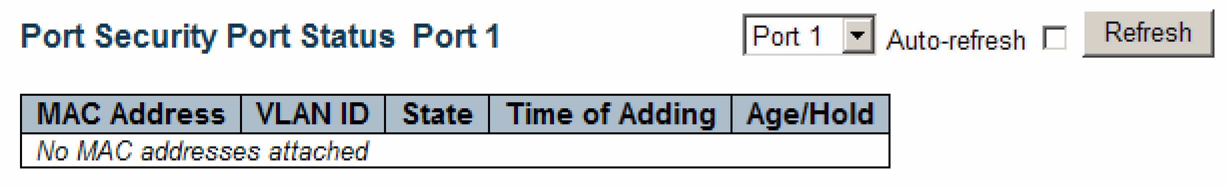
Port Status

Port	Users	MAC Count
1	-	-
2	-	-
3	-	-
4	-	-
5	-	-
6	-	-
7	-	-
8	-	-
9	-	-
10	-	-
11	-	-
12	-	-
13	-	-
14	-	-
15	-	-
16	-	-

Configuration	Description
User Module Name	The full name of a module that may request Port Security services.
Abbr	A one-letter abbreviation of the user module This is used in the Users column in the port status table.
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
MAC Count	Indicate the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be

	shown.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.3.1.1.2 Port



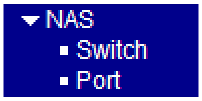
Port Security Port Status Port 1

Port 1 ▾ Auto-refresh □ Refresh

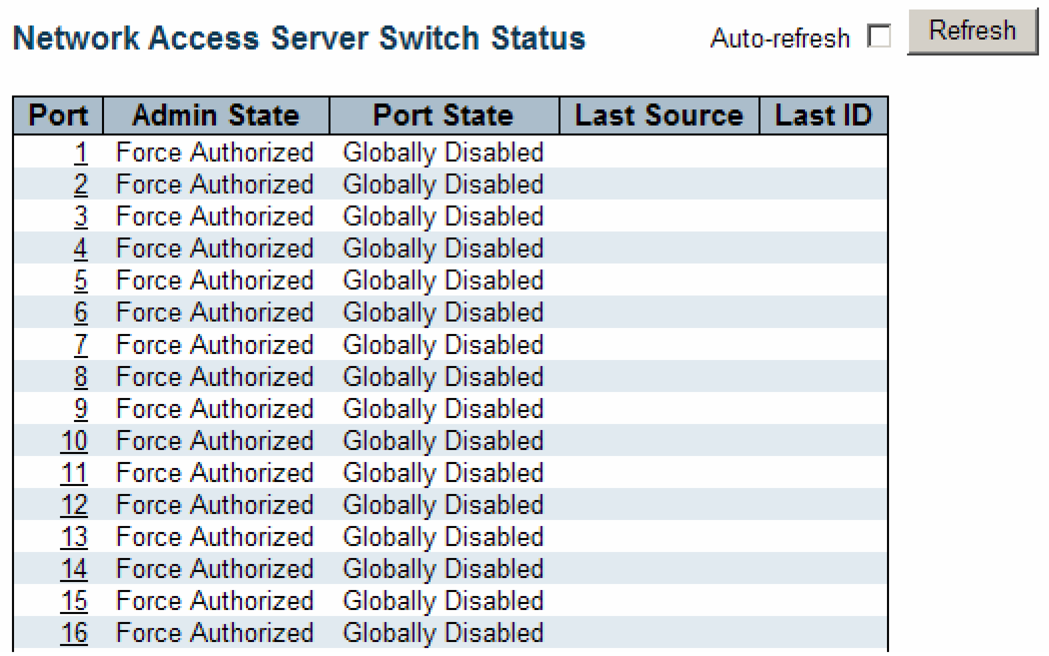
MAC Address	VLAN ID	State	Time of Adding	Age/Hold
No MAC addresses attached				

Configuration	**Description**
Port #	Select a port to display.
MAC Address	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating *"No MAC addresses attached"* is displayed.
VLAN ID	ditto
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Time of Adding	Show the date and time when this MAC address was first seen on the port.
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.3.1.2 NAS



3.3.1.2.1 Switch



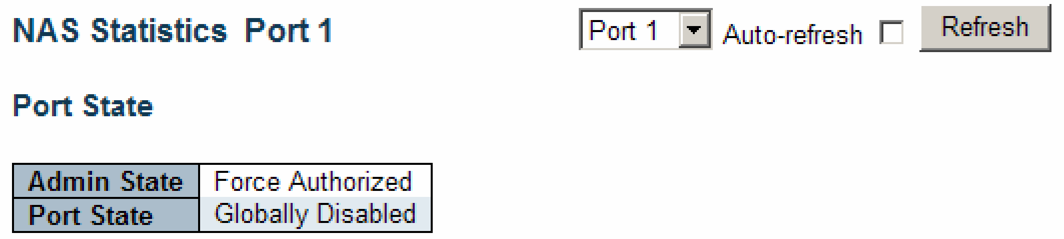
Network Access Server Switch Status

Auto-refresh □ Refresh

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		
7	Force Authorized	Globally Disabled		
8	Force Authorized	Globally Disabled		
9	Force Authorized	Globally Disabled		
10	Force Authorized	Globally Disabled		
11	Force Authorized	Globally Disabled		
12	Force Authorized	Globally Disabled		
13	Force Authorized	Globally Disabled		
14	Force Authorized	Globally Disabled		
15	Force Authorized	Globally Disabled		
16	Force Authorized	Globally Disabled		

Configuration	Description
Port #	Select a port to display.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.3.1.2.2 Port



NAS Statistics Port 1

Port 1 ▾ Auto-refresh □ Refresh

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Configuration	Description
Port #	Select a port to display the port state.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of

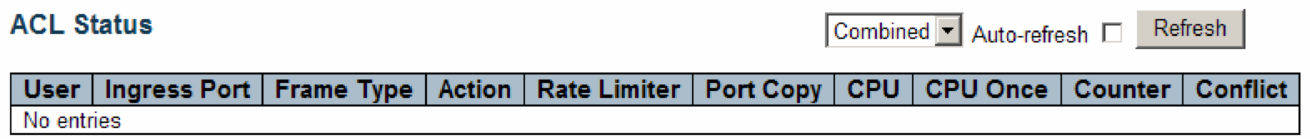
possible values.

Port State
The current state of the port. Refer to NAS Port State for a description of the individual states.

Auto-refresh
Check this box to enable an automatic refresh of the page at regular intervals.

Refresh
Click to refresh the page; any changes made locally will be undone.

3.3.1.3 ACL Status



User	Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	CPU	CPU Once	Counter	Conflict
No entries									

Configuration **Description**

User
Indicate ACL user.

Ingress Port
Indicate the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type
Indicate the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

Action
Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter
Indicates the rate limiter number of the ACE. The allowed range is ***1 ~ 15***. When “***Disabled***” is displayed, the rate limiter operation is disabled.

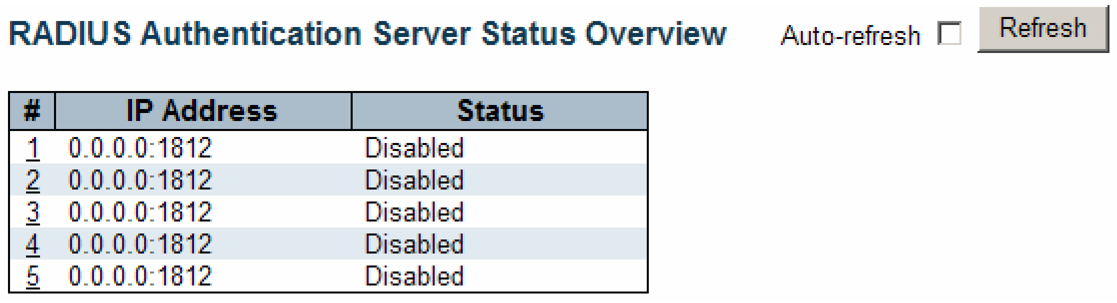
Port Copy
Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are ***Disabled*** or a ***specific port number***. When Disabled is displayed, the port copy operation is disabled.

CPU	Forward packet that matched the specific ACE to CPU
CPU Once	Forward the first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.3.2 Auth Server

3.3.2.1 RADIUS Overview



RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

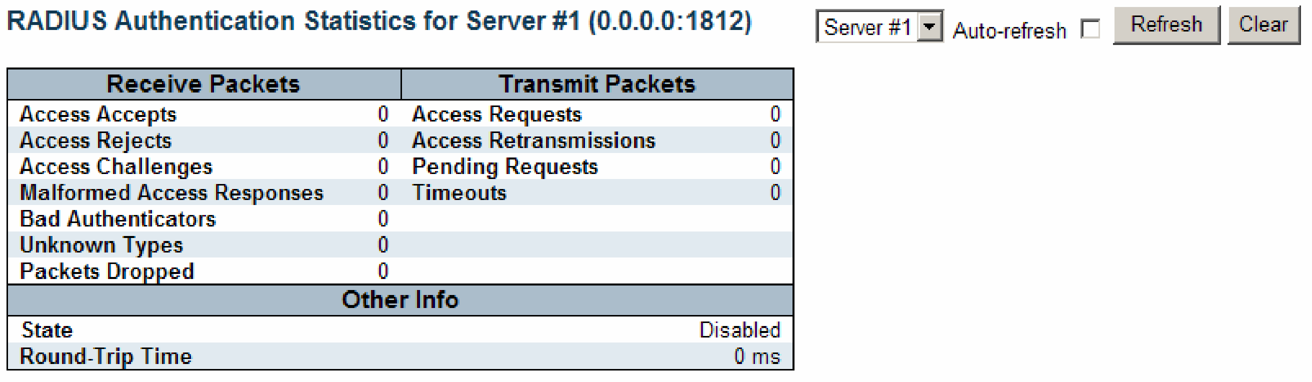
Configuration	**Description**
RADIUS Authentication Servers	
#	The RADIUS server number Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current state of the server This field takes one of the following values: ***Disabled:*** The server is disabled. ***Not Ready:*** The server is enabled, but IP communication is not yet up and running. ***Ready:*** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. ***Dead (X seconds left):*** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs

is displayed in parentheses. This state is only reachable when more than one server is enabled.

Auto-refresh — Check this box to enable an automatic refresh of the page at regular intervals.

Refresh — Click to refresh the page; any changes made locally will be undone.

3.3.2.2 RADIUS Details



RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
State	Disabled
Round-Trip Time	0 ms

Configuration — **Description**

Server # — Select a RADIUS server number.

Access Accepts — RFC4670 name: radiusAuthClientExtAccessAccepts
The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects — RFC4670 name: radiusAuthClientExtAccessRejects
The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges — RFC4670 name: radiusAuthClientExtAccessChallenges
The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses
RFC4670 name: radiusAuthClientExtMalformedAccessResponses
The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators — RFC4670 name: radiusAuthClientExtBadAuthenticators
The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types — RFC4670 name: radiusAuthClientExtUnknownTypes

The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Packets Dropped

RFC4670 name: radiusAuthClientExtPacketsDropped

The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests

RFC4670 name: radiusAuthClientExtAccessRequests

The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions

RFC4670 name: radiusAuthClientExtAccessRetransmissions

The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests

RFC4670 name: radiusAuthClientExtPendingRequests

The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts

RFC4670 name: radiusAuthClientExtTimeouts

The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

State

Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

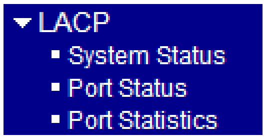
Round-Trip Time

RFC4670 name: radiusAuthClientExtRoundTripTime

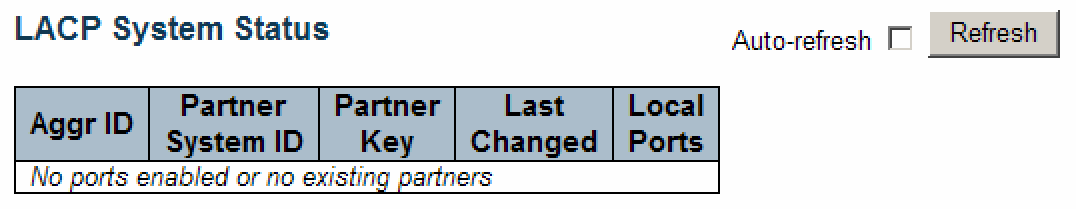
The time interval (measured in milliseconds) is between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear all counters.

3.4 LACP



3.4.1 System Status

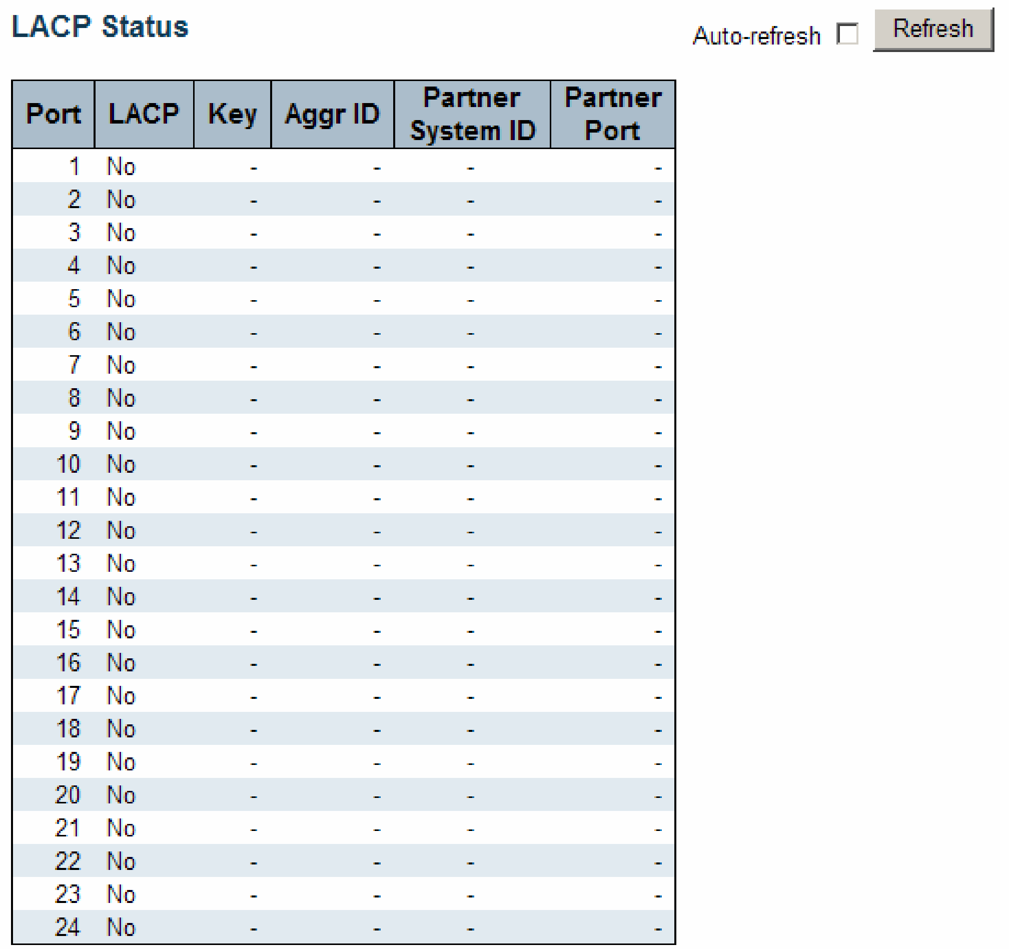

LACP System Status

Auto-refresh □ Refresh

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

Configuration	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last changed	The time since this aggregation changed.
Local Ports	Show which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.4.2 Port Status



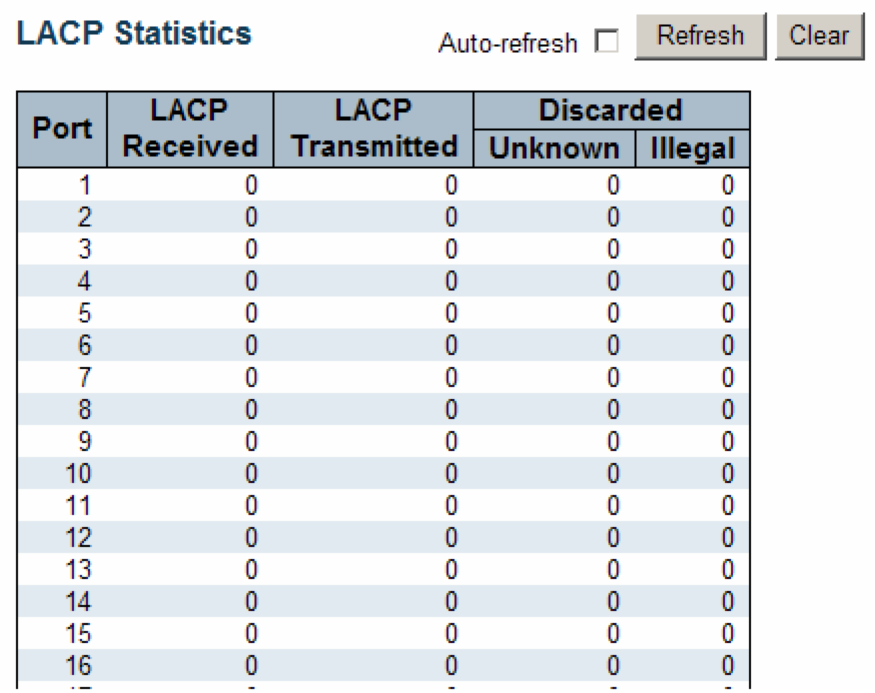
LACP Status

Auto-refresh □ Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-

Configuration	**Description**
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners port number connected to this port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.4.3 Port Statistics



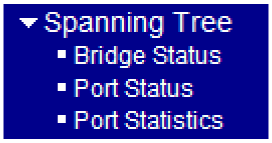
LACP Statistics

Auto-refresh □ Refresh Clear

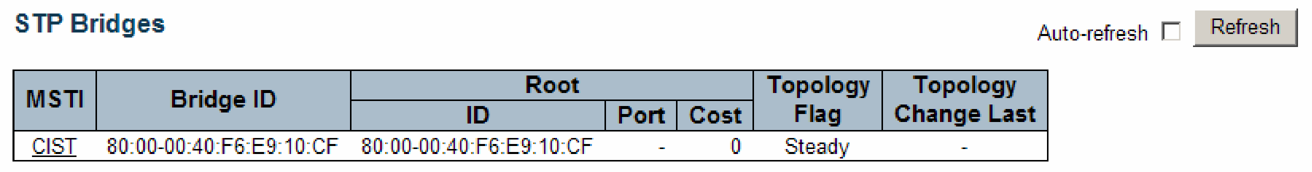
Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0

Configuration	Description
Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear all counters.

3.5 Spanning Tree



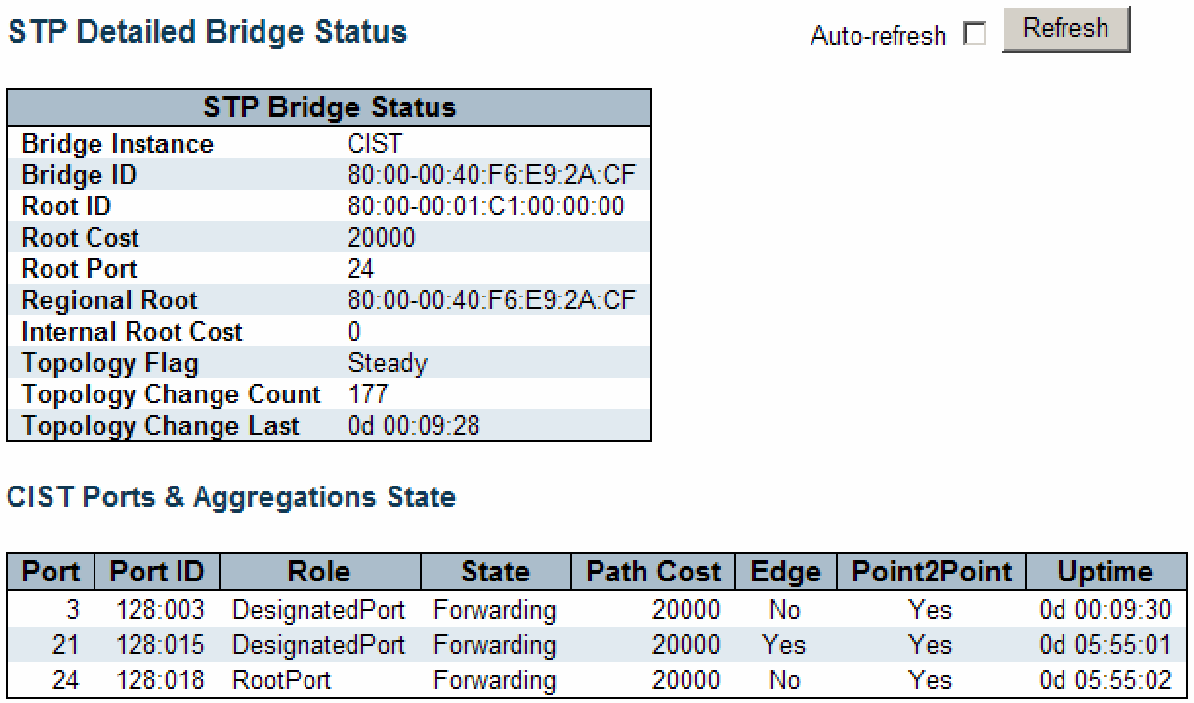
3.5.1 Bridge Status



STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:40:F6:E9:10:CF	80:00-00:40:F6:E9:10:CF	-	0	Steady	-

Configuration	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the *root* port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.



STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	80:00-00:40:F6:E9:2A:CF
Root ID	80:00-00:01:C1:00:00:00
Root Cost	20000
Root Port	24
Regional Root	80:00-00:40:F6:E9:2A:CF
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	177
Topology Change Last	0d 00:09:28

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point2Point	Uptime
3	128:003	DesignatedPort	Forwarding	20000	No	Yes	0d 00:09:30
21	128:015	DesignatedPort	Forwarding	20000	Yes	Yes	0d 05:55:01
24	128:018	RootPort	Forwarding	20000	No	Yes	0d 05:55:02

Configuration **Description**

Bridge Instance The Bridge instance - CIST, MST1, ...

Bridge ID The Bridge ID of this Bridge instance.

Root ID The Bridge ID of the currently elected root bridge.

Root Port The switch port currently assigned the *root* port role.

Root Cost Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. *(For the CIST instance only)*

Internal Root Cost The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. *(For the CIST instance only)*

Topology Flag The current state of the Topology Change Flag for this Bridge instance.

Topology Change Count The number of times where the topology-change flag has been set (during a one-second interval).

Topology Last The time passed since the Topology Flag was last set.

Physical Ports & Aggregations State

Switch ID The Switch ID of the logical port.

Port The switch port number of the logical STP port.

Port ID The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role — The current STP port role. The port role can be one of the following values: *AlternatePort, BackupPort, RootPort, DesignatedPort.*

State — The current STP port state. The port state can be one of the following values: *Blocking, Learning, Forwarding.*

Path Cost — The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge — The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

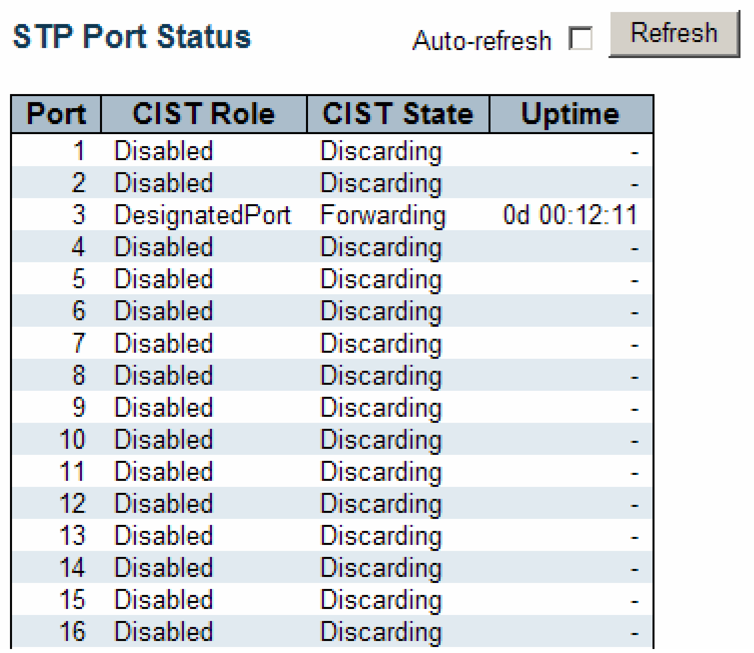
Point2Point — The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transition STP state.

Uptime — The time since the bridge port was last initialized.

Auto-refresh — Check this box to enable an automatic refresh of the page at regular intervals.

Refresh — Click to refresh the page; any changes made locally will be undone.

3.5.2 Port Status



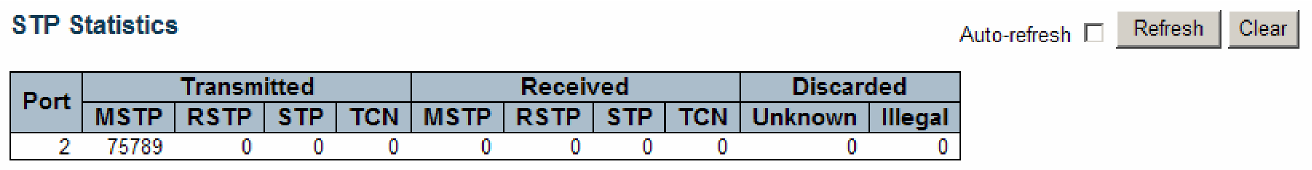
STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	DesignatedPort	Forwarding	0d 00:12:11
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	Disabled	Discarding	-
14	Disabled	Discarding	-
15	Disabled	Discarding	-
16	Disabled	Discarding	-

Configuration	Description
Port	The switch port number of the logical STP port.

CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: *AlternatePort*, *BackupPort*, *RootPort*, *DesignatedPort.*
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: *Blocking*, *Learning*, *Forwarding.*
Uptime	The time since the bridge port was last initialized.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.5.3 Port Statistics

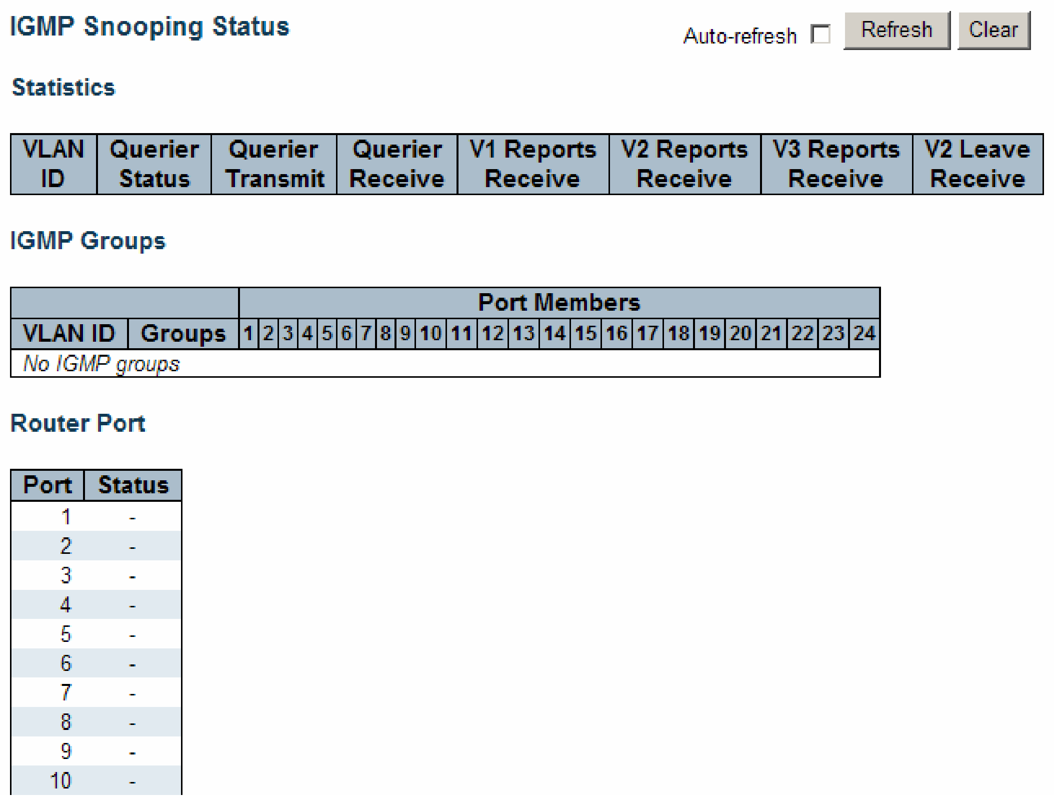


STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	75789	0	0	0	0	0	0	0	0	0

Configuration	**Description**
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page; any changes made locally will be undone.

3.6 IGMP Snooping



IGMP Snooping Status

Statistics

VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive

IGMP Groups

		Port Members																							
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
No IGMP groups																									

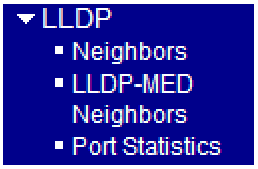
Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

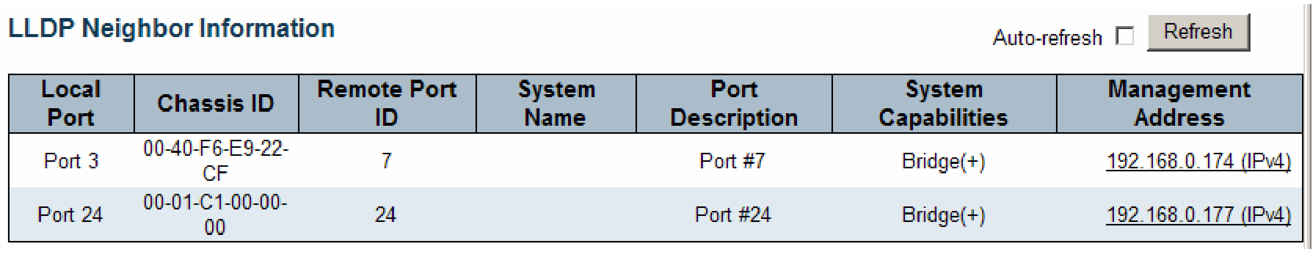
Status	Description
Statistics	
VLAN ID	The VLAN ID of the entry.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Transmit	The number of Transmitted Querier.
Querier Receive	The number of Received Querier.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.
IGMP Groups	
Groups	The present IGMP groups, Max. are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
Router Ports	
Port	The port number
Status	The port is a router port or not.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

Refresh	Click to refresh the page; any changes made locally will be undone.
Clear	Click to clear all counters.

3.7 LLDP



3.7.1 Neighbors



LLDP Neighbor Information

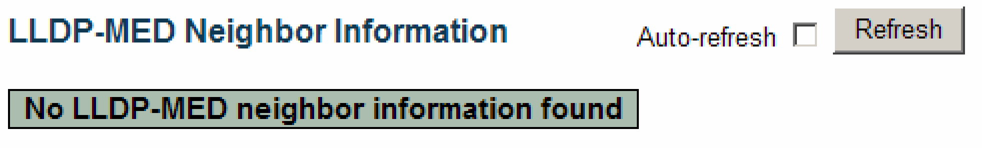
Auto-refresh □ Refresh

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 3	00-40-F6-E9-22-CF	7		Port #7	Bridge(+)	192.168.0.174 (IPv4)
Port 24	00-01-C1-00-00-00	24		Port #24	Bridge(+)	192.168.0.177 (IPv4)

Status	**Description**
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

Refresh	Click to refresh the page; any changes made locally will be undone.

3.7.2 LLDP-MED Neighbors


LLDP-MED Neighbor Information

No LLDP-MED neighbor information found

Status	Description
Port	The port on which the LLDP frame was received.
Device Type	LLDP-MED Devices are comprised of two primary **Device Types**: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** < LLDP-MED the using service communication IP in participate and edge, network LAN 802 IEEE at located are TIA-1057, defined as Devices, Endpoint> Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. Fore-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint

products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management

LLDP-MED Capabilities **LLDP-MED Capabilities** describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power vis MDI - PD
6. Inventory

7. Reserved

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The poosible application types are shown below.

***1. Voice* -** for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

***2. Voice Signaling* -** for use in network topologies that require a different policy for the voice signaling than for the voice media.

***3. Guest Voice* -** to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

***4. Guest Voice Signaling* -** for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

***5. Softphone Voice* -** for use by softphone applications on typical data centric devices, such as PCs or laptops.

***6. Video Conferencing* -** for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

***7. Streaming Video* -** for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

***8. Video Signaling* -** for use in network topologies that require a separate policy for the video signaling than for the video media.

Policy

Policy

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

TAG

TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged ot Untagged

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format

VLAN ID

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE

802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

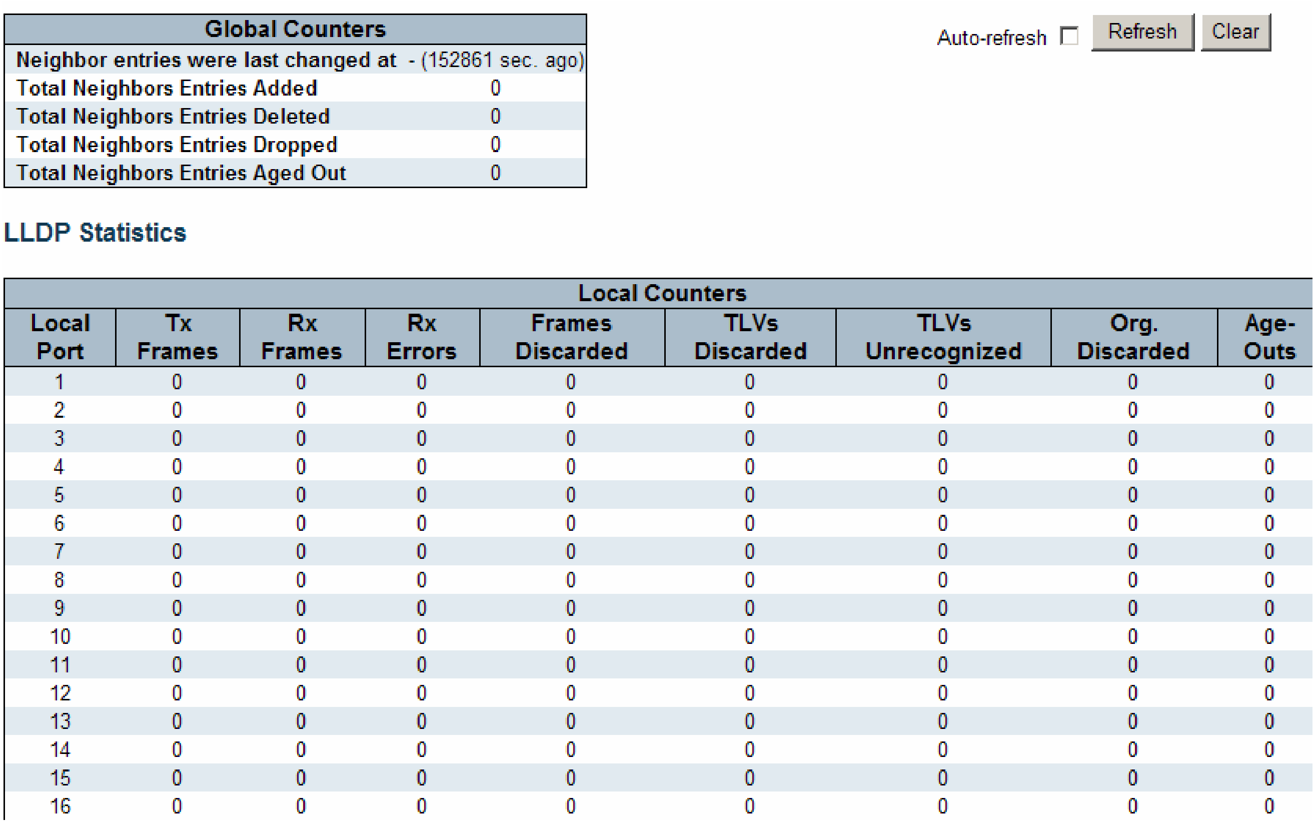
Priority — **Priority** is the Layer 2 priority to be used for the specified application type.One of eight priority levels (0 through 7)

DSCP — **DSCP** is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Auto-refresh — Check this box to enable an automatic refresh of the page at regular intervals.

Refresh — Click to refresh the page; any changes made locally will be undone.

3.7.3 Port Statistics



Global Counters	
Neighbor entries were last changed at	- (152861 sec. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0

Global Status — **Description**

Neighbor entries were last changed at

Shows the time of the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.

Total Neighbors Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped

Shows the number of LLDP frames dropped due to that the entry table was full.

Total Neighbors Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

Local Port — The port on which LLDP frames are received or transmitted.

Tx Frames — The number of LLDP frames transmitted on the port.

Rx Frames — The number of LLDP frames received on the port.

Rx Errors — The number of received LLDP frames containing some kind of error.

Frames Discarded — If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded — Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized — The number of well-formed TLVs, but with an unknown type value.

Org. Discarded — The number of organizationally TLVs received.

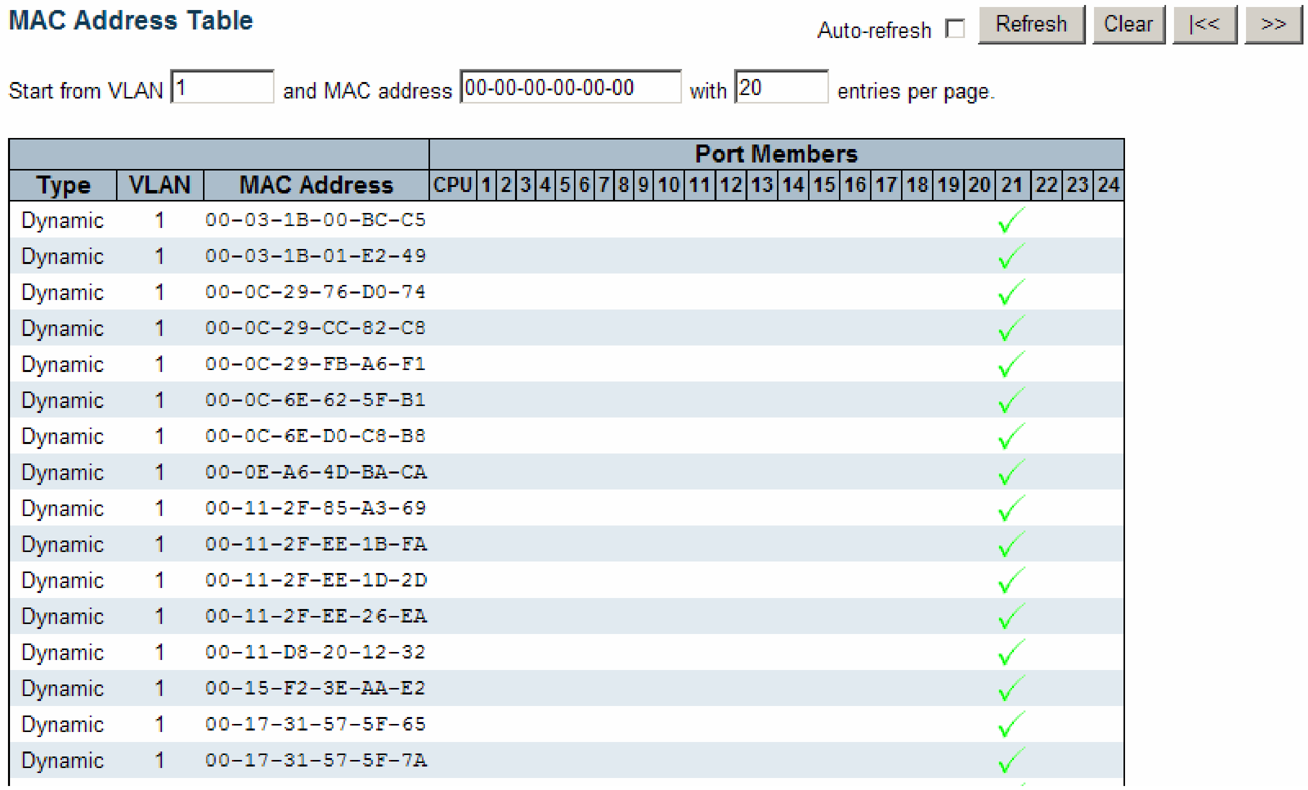
Age-Outs — Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Auto-refresh — Check this box to enable an automatic refresh of the page at regular intervals.

Refresh — Click to refresh the page; any changes made locally will be undone.

Clear — Click to clear all counters.

3.8 MAC Table



MAC Address Table

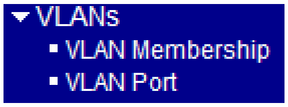
Auto-refresh □ Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members																								
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Dynamic	1	00-03-1B-00-BC-C5																						✓			
Dynamic	1	00-03-1B-01-E2-49																						✓			
Dynamic	1	00-0C-29-76-D0-74																						✓			
Dynamic	1	00-0C-29-CC-82-C8																						✓			
Dynamic	1	00-0C-29-FB-A6-F1																						✓			
Dynamic	1	00-0C-6E-62-5F-B1																						✓			
Dynamic	1	00-0C-6E-D0-C8-B8																						✓			
Dynamic	1	00-0E-A6-4D-BA-CA																						✓			
Dynamic	1	00-11-2F-85-A3-69																						✓			
Dynamic	1	00-11-2F-EE-1B-FA																						✓			
Dynamic	1	00-11-2F-EE-1D-2D																						✓			
Dynamic	1	00-11-2F-EE-26-EA																						✓			
Dynamic	1	00-11-D8-20-12-32																						✓			
Dynamic	1	00-15-F2-3E-AA-E2																						✓			
Dynamic	1	00-17-31-57-5F-65																						✓			
Dynamic	1	00-17-31-57-5F-7A																						✓			

MAC Table Column	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to updates the information, starting from the current entry ID.
Clear	Click to clear all counters.
I <<	Updates the system log entries, starting from the first available entry ID.
>>	Updates the system log entries, starting from the last entry currently displayed.

3.9 VLAN



3.9.1 VLAN Membership

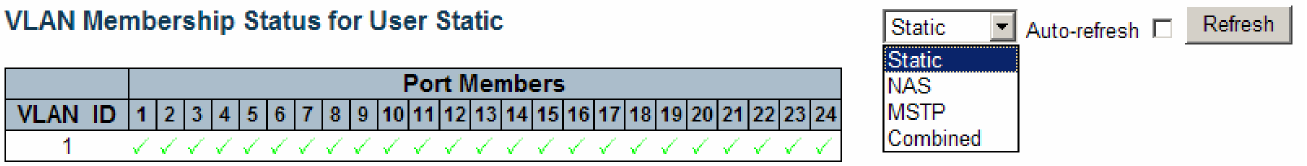
A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN:

Static: CLI/Web/SNMP users

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MSTP: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users is selected, it shall show this information for all the VLAN Users, and this is the default. VLAN membership allows the frames Classified to the VLAN ID to be forwarded to the respective VLAN member ports.



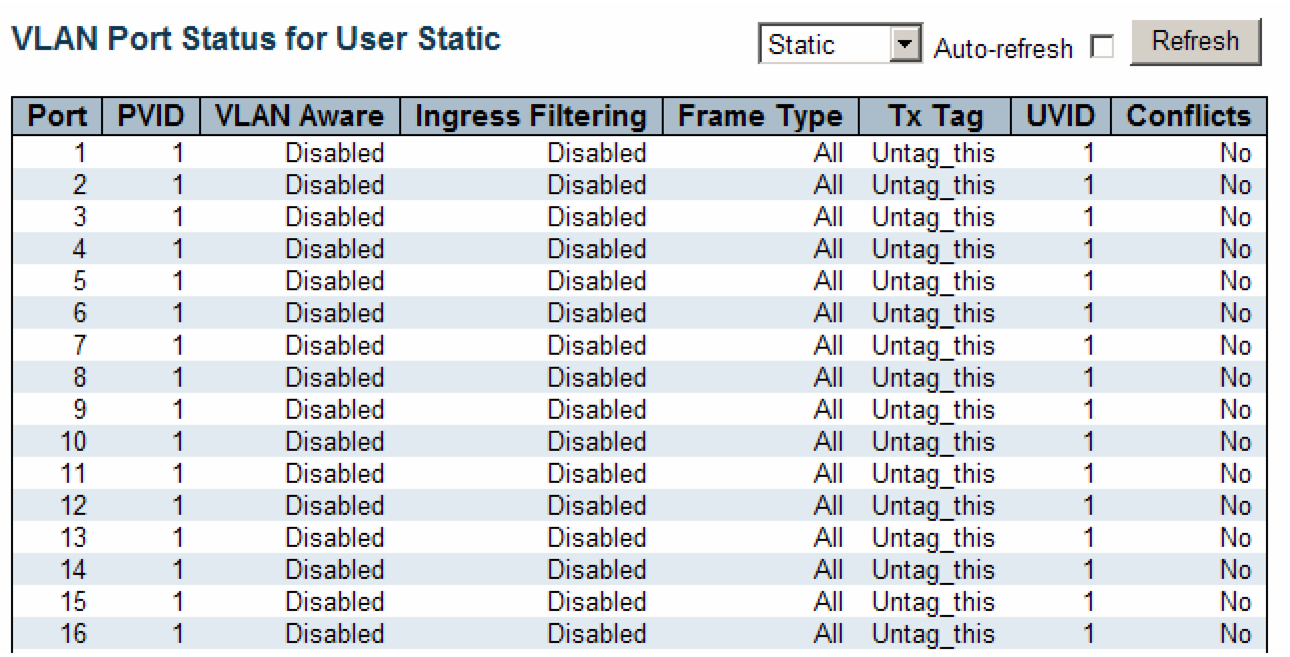
VLAN Membership Status for User Static

	Port Members																							
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Static ▾ Select a type of VLAN Users

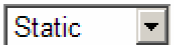
Status	Description
VLAN ID	Indicates the ID of this particular VLAN.
Port Members	A row of check marks is displayed for each VLAN ID. The port with check mark is the member of the associated VLAN ID.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to updates the information, starting from the current entry ID.

3.9.2 VLAN Port



VLAN Port Status for User Static

Port	PVID	VLAN Aware	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	Disabled	Disabled	All	Untag_this	1	No
2	1	Disabled	Disabled	All	Untag_this	1	No
3	1	Disabled	Disabled	All	Untag_this	1	No
4	1	Disabled	Disabled	All	Untag_this	1	No
5	1	Disabled	Disabled	All	Untag_this	1	No
6	1	Disabled	Disabled	All	Untag_this	1	No
7	1	Disabled	Disabled	All	Untag_this	1	No
8	1	Disabled	Disabled	All	Untag_this	1	No
9	1	Disabled	Disabled	All	Untag_this	1	No
10	1	Disabled	Disabled	All	Untag_this	1	No
11	1	Disabled	Disabled	All	Untag_this	1	No
12	1	Disabled	Disabled	All	Untag_this	1	No
13	1	Disabled	Disabled	All	Untag_this	1	No
14	1	Disabled	Disabled	All	Untag_this	1	No
15	1	Disabled	Disabled	All	Untag_this	1	No
16	1	Disabled	Disabled	All	Untag_this	1	No



Select a type of VLAN Users

Status	Description
Port	The logical port for the settings contained in the same row.
PVID	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
VLAN Aware	Shows the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress Filtering	Show the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
Frame Type	Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Tx Tag	Shows egress filtering frame status whether tagged or untagged.
UVID	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
Conflicts	Shows status of Conflicts whether exists or Not. When a Volatile VLAN User

requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

1. Functional Conflicts between feature.

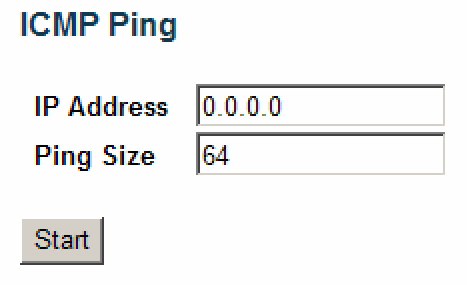
2. Conflicts due to hardware limitation.

3. Direct conflict between user modules.

---

4. Diagnostics

4.1 Ping



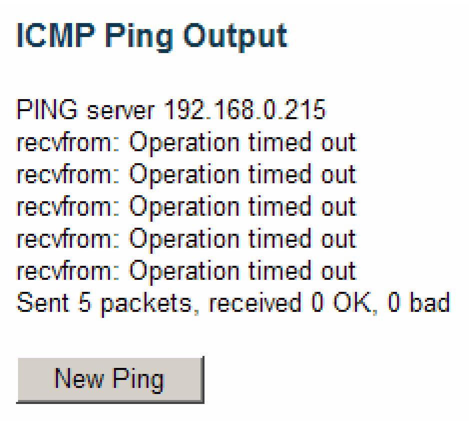
ICMP Ping

IP Address: 0.0.0.0

Ping Size: 64

Settings	Description
IP Address	The destination IP Address
Ping Size	Payload size of the ICMP packet. Values range: *8* ~ *1400* bytes.
Start	Click to start ping test. Five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

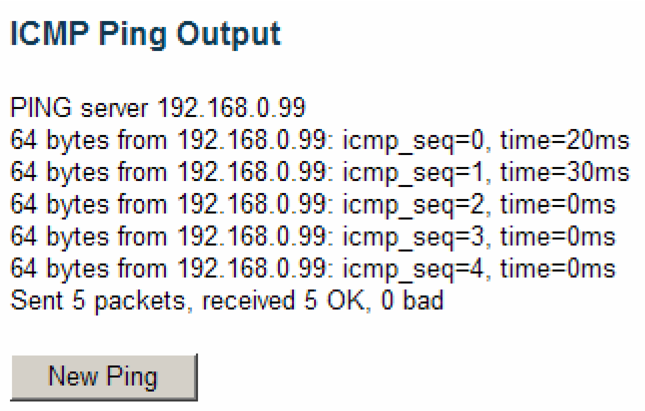
Result displayed for a failed ping test



ICMP Ping Output

```
PING server 192.168.0.215
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
```

Result displayed for a successful ping test

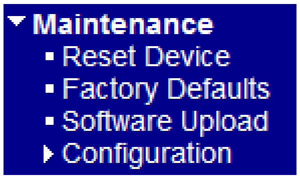


ICMP Ping Output

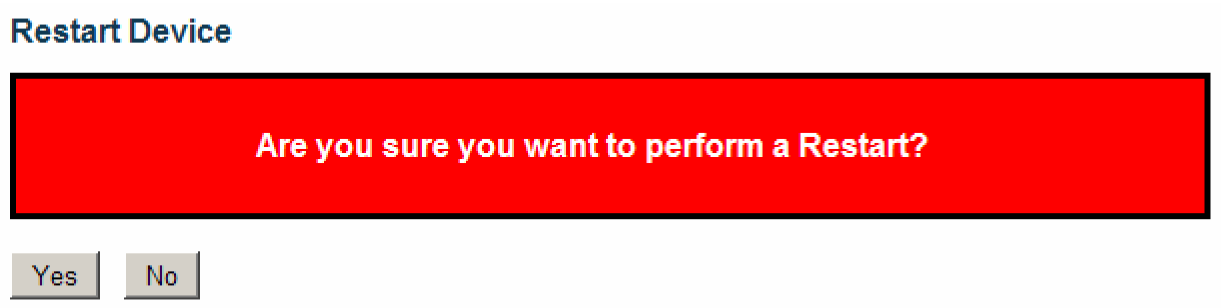
```
PING server 192.168.0.99
64 bytes from 192.168.0.99: icmp_seq=0, time=20ms
64 bytes from 192.168.0.99: icmp_seq=1, time=30ms
64 bytes from 192.168.0.99: icmp_seq=2, time=0ms
64 bytes from 192.168.0.99: icmp_seq=3, time=0ms
64 bytes from 192.168.0.99: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

New Ping	Click to start a new ping test.

5. Maintenance



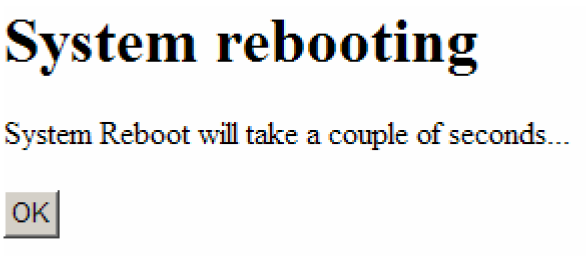
5.1 Reset Device



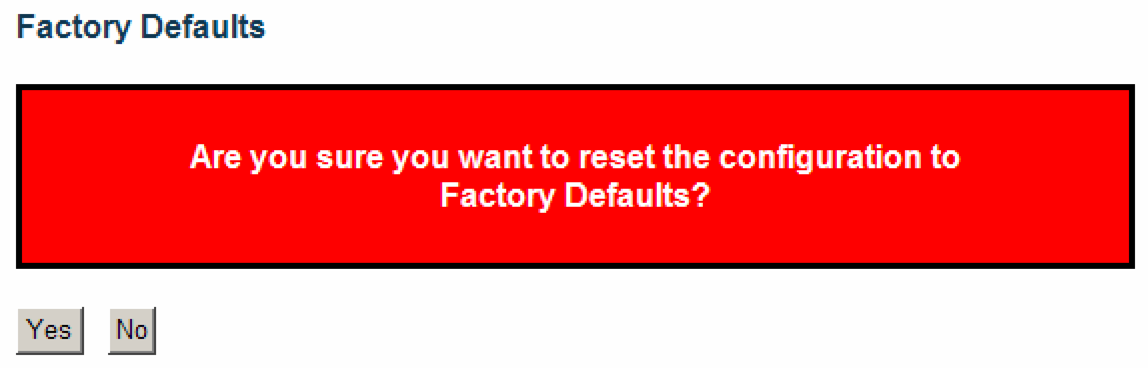
Restart Device

Are you sure you want to perform a Restart?

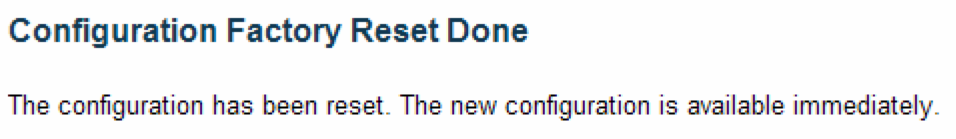
You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices.

Yes	Click to reboot device. "System rebooting" message is displayed as follows.  System rebooting System Reboot will take a couple of seconds... OK
No	Click to return to the Port State page without rebooting.

5.2 Factory Defaults

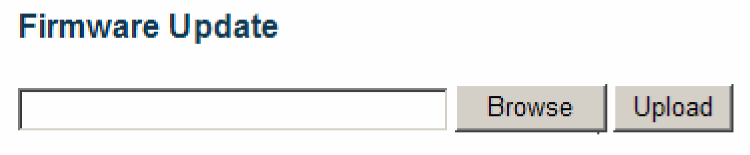

Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Yes	Click to reboot device. “System rebooting” message is displayed as follows.  Configuration Factory Reset Done The configuration has been reset. The new configuration is available immediately.
No	Click to return to the Port State page without rebooting.

5.3 Software Upload

This page facilitates an update of the firmware controlling the switch.

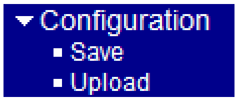

Firmware Update

Browse	Click to the location of a software image
Upload	Click to start uploading.

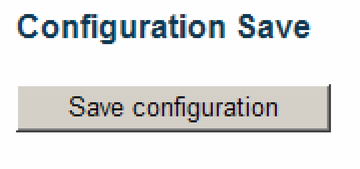
After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch reboots.

Warning**: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress.* ***Do not reset or power off the device at this time *or the switch may fail to function afterwards.*

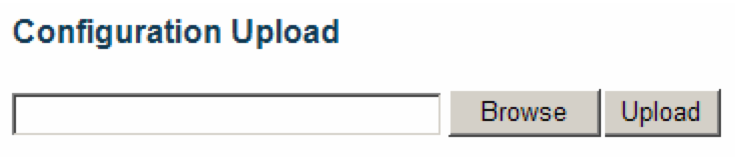
5.4 Configuration



You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags: Header tags: <?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.


Configuration Save

Save configuration	Click to start download of the configuration.


Configuration Upload

Browse	Click to the location of a configuration file
Upload	Click to start uploading configuration.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Use multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation*, *Link Aggregation*).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a

MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DDM

DDM is an acronym for Digital Diagnostics Monitoring. Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agent¡¦s MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EPS

EPS Is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol, is used for network discovery, and works by having the units in the network exchanging information with their neighbors using LLDP frames.

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

N

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality.

MEP functionality like CC and RDI is based on this

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

P

PD

PD is an acronym for Powered Device. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

`ping` uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

There are 4 web-pages associated with the QoS configuration:

QoS|QoS Control List: The web page shows the QCEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one QCE even though there are more matching QCEs. The first matching QCE will give that frame a priority: Low, Normal, Medium or High. 5 different QCLs can be created, each with 8 different QCEs. You assign each port a QCL id under QoS|Ports page. The QoS counters can be viewed under Monitor|Ports|QoS statistics. There are number of parameters that can be configured with a QCE. Read the Web page help text to get further information for each of them.

QoS|Ports: The Ports QoS page is used to assign a QCL id to an ingress port. Furthermore you can assign a default class to a port and a queuing mode. Strict queuing means that the higher priority frame will always be served before a lower priority frame. Weighted priority will give each class some weight of the bandwidth.

QoS|Rate Limiters: Under this page you can configure the policer (ingress) and shaper (egress) rate for each port. See the help page for details.

QoS|Storm Control: Here you can limit the flooding in the switch, i.e. the rate you choose applies to the whole switch. Choose the mix of Unicast, Multicast and Broadcast storm control. See the help page for details.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of arp.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

Virtual LAN: a method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

W

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages use radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WTR

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.